# CRYPTYK:

# A Hybrid Decentralized Architecture for Enterprise Security and Storage

Adam Weigold, Ph.D.
Cryptyk Inc.
adam@cryptyk.com

Raghunadha Kotha, M.S.
Cryptyk Inc.
raghu@cryptyk.com

Daniel Floreani, Ph.D.
Cryptyk Inc.
daniel@cryptyk.com

November 2017

## Abstract

The CRYPTYK platform is a hybrid decentralized data processing architecture designed for secure, scalable management of online data storage, file sharing, document editing, user access, email, messaging and other cloud-based applications within businesses, enterprises, government organizations and for individual consumers. This decentralized technology designed by Cryptyk Inc utilizes CRYPTYK Tokens (or CTKs) to power an open source cyber-security platform benefitting all industries that are susceptible to cyber-security breaches including banking, finance, law, insurance, healthcare, transport, logistics, media, construction and government. This technology seeks to displace single source Cloud Storage Providers (CSPs), Cloud Access Security Brokers (CASBs), Cloud Security Gateways (CSGs), Storage Partitions, Anti-Virus Scanners, Threat Monitors and other security products. The CRYPTYK ecosystem manages security for data-at-rest (storage), data-in-motion (email / chat / payments) and data-in-use (file editing / sharing / collaboration). The ecosystem is structured to provide scalable benefits and incentives for all participants to grow the security, integrity, financial competitiveness and performance of Cryptyk technology for the benefit of the CRYPTYK token or CTK value (and hence all its participants). Blockchain based networks that use a large number of consensus driven processing nodes are ideal for managing network security. However, they are not well suited for managing file storage and sharing applications because of inherent latencies of the order of tens of seconds or more. Instead of storing files on a consensus-driven node structured blockchain network, the CRYPTYK ecosystem uses a low latency, decentralized cloud platform with multiple dedicated cloud storage providers as file storage nodes. In addition to a decentralized multi-cloud platform for file storage, the hybrid ecosystem integrates a private blockchain platform for a secure immutable record of all user access sessions and file transactions. This double-decentralized platform uses the CRYPTYK digital token to drive all of its blockchain components, pay for its development, and generate revenues from its security and storage services. This design architecture meets the security, performance, compliance, speed, cost and usability requirements for managing all forms of confidential data between business enterprises, their employees and their customers. It also provides for the secure and cost-efficient transfer of confidential data between allied or federated enterprises and benefits individual consumers with free storage and security services.

## 1. Introduction

Enterprises are increasingly storing more of their confidential data online via cloud storage vendors. They are also increasingly using online applications that run on the cloud to create, collect, manage, use and sell information for business management operations. The advantages of the cloud to any business or enterprise include greater employee mobility, reduced operational costs and the elimination of capital expenses for storage hardware. However the biggest risk, largest cost and major operational concern involved in migrating an enterprise to the cloud is security. While cloud storage costs may have dropped to very low commodity level pricing (around $5 - $10 per TB / user / month), enterprise-class security remains an expensive premium priced service (around $40 - $80 / user / month). Moreover, cloud security technologies are very incomplete and imperfect solutions. This explains why global cyber-security losses are now approaching $1 trillion annually[1] despite a global cyber-security industry worth over $100 billion[2]. Existing security technologies may act to reduce the risk of security breaches but they do not mitigate the risk entirely. Over time all cloud storage vendors will eventually be compromised, and all information stored by enterprises in the cloud will eventually be exposed to security breaches.

The fundamental weakness of existing cloud storage and enterprise security technologies lies in their centralized design architecture that relies on trusted third-party vendors. Every cloud storage vendor is vulnerable to cyber-security attacks, and once a security breach has been successfully achieved enormous amounts of confidential data can be readily stolen from a centralized network. We can identify the five main security threats to enterprise networks:

(1) External threats from remotely located syndicated hacker groups.
(2) Viral threats from malicious software programs such as viruses, malware and ransomware.
(3) Operational failure threats and denial of service attacks.
(4) Internal threats from bad actors, disgruntled employees.
(5) Surveillance intercept threats or man-in-the-middle attacks.

To counter these five security threats an enterprise can invest in a complex, expensive combination of:

- Cloud Access Security Brokers (CASBs) or Cloud Security Gateways (CSGs) that monitor and control user / employee access to cloud storage and cloud application services,
- Data Leak Prevention (DLP) and Threat Analysis products that analyze user access and the sharing of files to minimize potential insider threats and data losses due to human error,
- Multi-Factor Authorization (MFA) login tools that verify the identity of users / employees,
- Firewalls and Partitions that act to prevent or minimize unauthorized access from external sources to confidential files and data,

- Anti-Virus and Spyware Software that scan for hazardous black-listed viruses, malware and ransomware, and
- Encryption and tokenization tools such that use cryptographic data encoding algorithms with public/private keys to protect and audit data-at-rest and data-in-motion assets.

The total cost of a complete enterprise-class security solution for cloud applications can typically vary from between $40 and $80 / user / month and this is the major cost factor when determining cloud adoption strategy[3]. Nonetheless, most large enterprises who adopt these conventional cloud security solutions will still suffer significant losses due to security breaches every year.

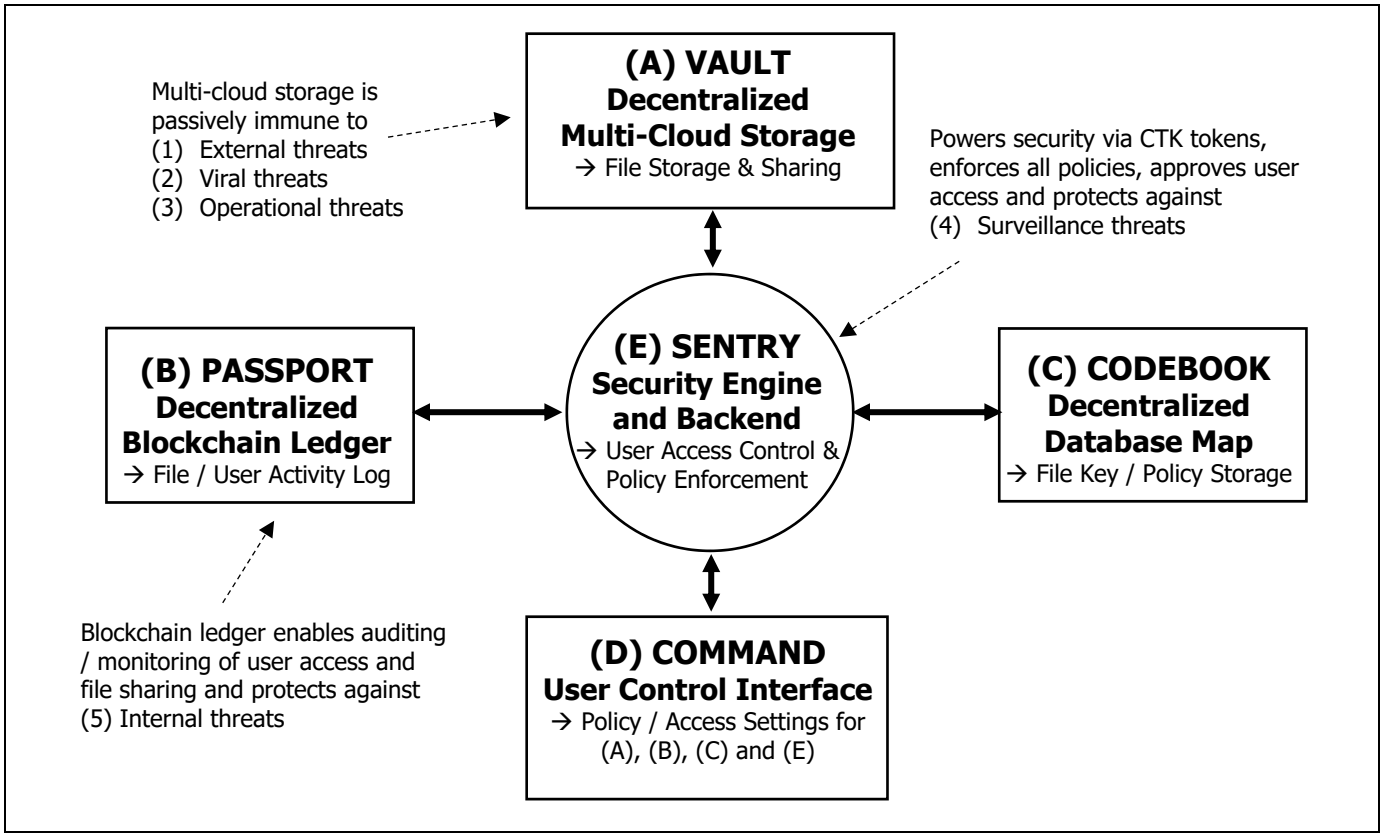
In contrast to conventional centralized enterprise security and storage technologies, the CRYPTYK platform presented here describes a decentralized data management architecture designed for highly secure, scalable control of data storage, data management, file sharing, file editing, user access, emails, and data compliance. While there exist other decentralized file storage platforms based on blockchain technology such as Sia[4] and Filecoin[5], the hybrid CRYPTYK platform described here does not suffer the inherent latency problems of blockchain-only storage technologies. Existing blockchain storage technologies typically demonstrate large access latencies in excess of 10 – 20 seconds and as much as several minutes or more. This effectively makes real-time file management, data-in-use and data-in-motion applications too slow and unusable for multi-user enterprise environments. Hence existing blockchain-based file storage technologies are primarily focused on individual, libertarian minded public consumers who want to upload large files as opposed to large file numbers. Blockchain-only storage simply doesn't meet the security, performance, latency and usability requirements for enterprise customers. Conversely the CRYPTYK hybrid blockchain technology developed by Cryptyk Inc has demonstrated highly usable access latencies less than 200msec while also offering vastly reduce attack surfaces to hackers for a more diverse range of file-types compared to blockchain-only platforms[6].

Moreover, the CRYPTYK ecosystem provides much more than a secure, usable, low-latency file storage platform for enterprise environments. It also manages user access control, file tracking / logging / auditing, email / chat security, internal threat monitoring, policy enforcement and industry / legal compliance. The ecosystem represents a simple, complete enterprise security and storage solution that protects a business, organization or enterprise against all five main cyber-security threats (or attack vectors) of migrating to the cloud. As a complete enterprise security and storage solution in a single product bundle for enterprise customers, the CRYPTYK ecosystem can displace many conventional cyber-security and storage technologies. Most importantly of all, the unique crypto-economics of the CRYPTYK ecosystem means that the individual customers of every Cryptyk enterprise customer ultimately become Cryptyk customers themselves via document sharing actions by the enterprise.

Consequently, this spreads the wider adoption throughout the business and enterprise community via follow-up adoption by their individual customers or public consumers. This is an example of the network effect of a crypto-economy that aligns both participant incentives with technology growth to realize viral adoption and customer migration.

The CRYPTYK ecosystem incentivizes enterprise customers with a complete security solution, simpler deployment, easier management and lower overall costs. The platform addresses the security problem at the fundamental data storage level itself, thereby not requiring the complex, piecemeal, after-thought approaches of conventional security and storage solutions. Security encryption is written into the decentralized storage process for passive protection of file storage. There are also inherent benefits for the enterprises' customers (ie: the individual public consumer) with limited free storage and security services provided by the enterprise. The ecosystem further incentivizes the processing of information for CRYPTYK token participants (or CTK miners) with rewards for verifying user ID, file uploads, file sharing, data integrity and secure user access sessions. It also incentivizes the open-source development of future platform features and encourages rapid trial and adoption by all customers. In terms of architecture, the hybrid platform consists of three different but complimentary decentralized platforms integrated with a security engine and user-interface to form a complete security and storage solution.

**Figure 1: Overview of the CRYPTYK Hybrid Security and Storage Platform**



Specifically, as detailed in Figure 1, the CRYPTYK platform comprises of (A) a decentralized, multi-vendor cloud storage platform called VAULT for encrypted file storage and file sharing, (B) a decentralized blockchain platform called PASSPORT for immutable storage of all user access sessions and file transactions, (C) a decentralized database map for storage of file encryption keys, transaction data and audit logs, (D) a user control interface called COMMAND for managing file storage / sharing, security policies, user access and file permissions, and (E) a central security engine and backend called SENTRY for the integration of all platform components and the enforcement of security policies, user access controls, file settings, participant incentives and the Cryptyk Token ecosystem.

All three decentralized storage platforms (multi-cloud, blockchain and database) interact with each other via the SENTRY security engine to perform complementary tasks for the benefit of all participants in the CRYPTYK ecosystem. They also protect against different types of security threats in various manners to provide an enterprise customer with a complete data security and storage solution against all five potential security threats. In summary, the CRYPTYK platform and CTK ecosystem is a complete enterprise security and storage solution that leverages a viral network effect among enterprises and their consumers to increase the adoption, performance, security and value of the platform for all participants.

## 2. Technical Background and Challenges

While decentralized platforms offer significant potential benefits for enterprise customers and users in terms of security and scalable throughput, the exact design and size of a decentralized platform can dramatically affect numerous other product performance and usability characteristics for the user. Of particular relevance is how the type and number of storage nodes (or information processing nodes) can affect both the potential attack surface and access latency of the platform. In addition, migrating confidential data from a centralized architecture to a decentralized architecture should typically benefit enterprise customers in terms of cost-effectiveness. Despite the potential of improved platform security, widespread adoption of a decentralized security and storage platform is highly challenging unless there exists significant cost savings for the paying enterprise customer. Consequently, identifying the sweet spot in terms of node number, attack surface, latency and cost benefit is critical to the optimal design of a decentralized network solution.

## 2(a). Attack Surface in Decentralized Systems

A file or data payload that is divided into smaller portions that are distributed across a decentralized storage platform is inherently more secure than data stored on a centralized single vendor storage platform. In principle, the greater the number of storage nodes (and hence greater degree of decentralization) the

smaller the potential attack surface of the storage platform. The attack surface is usually defined as the sum of all possible attack vectors (or cyber-security threats). Let us first define the *relative* attack surface ($AS_n$) of a storage platform with $n$ nodes as the attack surface given as a normalized fraction of the maximum possible attack surface (ie: equal to 1). Let us also assume that the relative attack surface for all five individual attack vectors against a single storage node (ie*:* $n = 1$) are identical, as follows:

$$AS_1 \text{ (maximum)} = AS_1 \text{ (a+b+c+d+e)} = 1$$

$$AS_1 \text{ (a)} = AS_1 \text{ (b)} = AS_1 \text{ (c)} = AS_1 \text{ (d)} = AS_1 \text{ (e)} = 0.2$$

Now let us take the simple example of a single source storage vendor that is fully protected against all potential attack vectors except from external threats. In this case;

$$AS_1 \text{ (a)} = 0.2 \text{ and } AS_1 \text{ (b)} = AS_1 \text{ (c)} = AS_1 \text{ (d)} = AS_1 \text{ (e)} = 0$$

$$AS_1 \text{ (total)} = AS_1\text{(a)} = 0.2 = 1/5$$

If a file is instead divided into two smaller portions and stored across two identical storage nodes (ie: $n = 2$) then both storage nodes are required to be compromised for a security breach to be successful. In this case the relative attack surface of the storage platform is equal to the product of the attack surfaces of the individual nodes, as follows;

for n = 2 $\quad AS_2 \text{ (total)} = AS_1 \text{ (a)} \times AS_1 \text{ (a)} = 0.04 = 1 / 25 = 1 / 5^2$

and for n = 3, $\quad AS_3 \text{ (total)} = AS_1 \text{ (a)} \times AS_1 \text{ (a)} \times AS_1 \text{ (a)} = 0.008 = 1 / 125 = 1 / 5^3$

In general, if each storage node has a relative attack surface equal to $AS_1$ then the relative attack vector for a $n$-node storage platform as a whole is equal to;

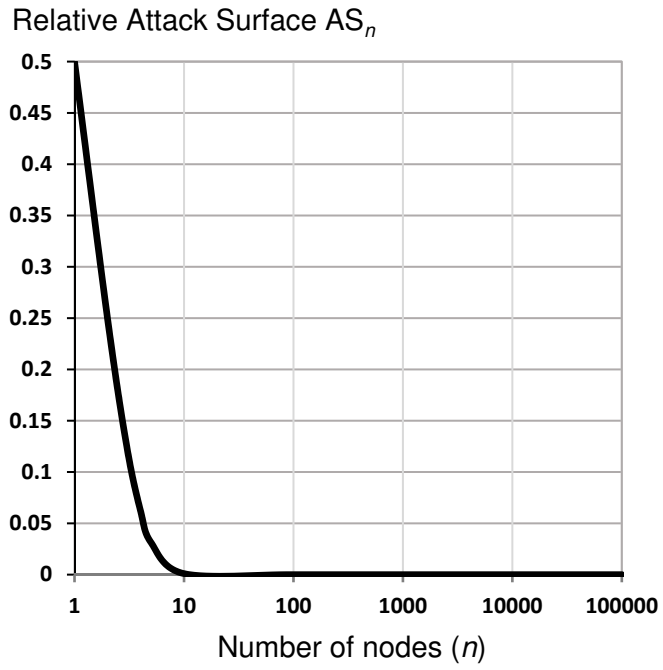
$$AS_n = ( AS_1 )^n$$

Now if we take the simplest example where the total relative attack surface for a single node is equal to 50% (ie: $AS_1 = 0.5$) then the relative attack surface for a $n$-node platform is equal to;

$$AS_n = ( 0.5 )^n$$

Figure 2a (right) shows the highly asymptotic behavior of the relative attack surface with

**Figure 2a: Attack Surface vs Node Number**



increasing node number for this example of $AS_1 = 50\%$. A dramatic reduction of the relative attack surface to less than 4% can be achieved with the use of only 5 storage nodes. The relative attack surface drops further to around 0.1% for 10 nodes, and to less than 0.0001% for 100 nodes. Beyond 100 storage nodes the attack surface becomes infinitesimally small approaching zero.

Consequently, the vast majority of potential reduction in a decentralized platforms attack surface can be achieved with a limited amount of decentralization using a relatively small number of distributed independent storage nodes (ie: $n = 5 - 10$). Critical to the design of the CRYPTYK cloud storage platform (ie: VAULT) is the large improvement in security levels that is possible with only 5 to 10 storage nodes.

## 2(b). Latency in Decentralized Systems

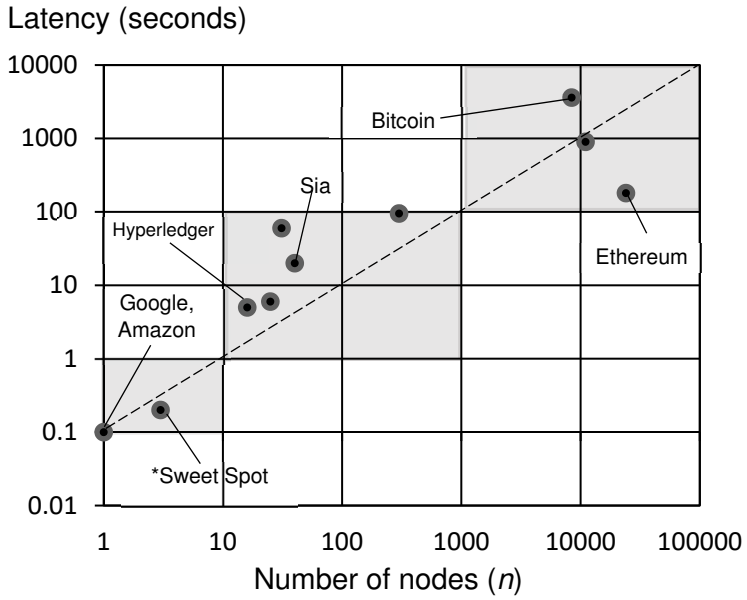
Conventional centralized storage platforms such as Google Drive, Amazon S3 and iCloud and other content delivery networks exhibit very low access latency while still delivering reasonable throughput speeds for data upload and download. Access latency is an important performance and usability issue for real-time applications requiring the frequent upload, download and management of lots of small sized files (typically < 1MB). Online cloud-based applications such as file / folder management, file sharing and live editing generally demand access latencies no larger than a few hundred microseconds to be considered usable in real-time. Regardless of the upload or download speed of a storage platform (ie: throughput), large multi-second access latencies can render real-time file storage, management and editing applications unusable for most users. Most consumers and users of cloud bases storage platforms do not want to wait tens of seconds or more to initiate the upload of a small file that may take less than a second to upload via conventional cloud storage services. Consequently, existing centralized storage systems with high throughput and low latency are better suited to real-time online file storage, management and editing applications. They only suffer one major problem in that they exhibit large potential attack vectors and poor data security characteristics.

Conversely, decentralized blockchain storage platforms such as Sia[3] and Filecoin[4] are ideal for the upload or download of very large files and data payloads (ie: > 100MB). Decentralized platforms can be configured to exhibit improved data security, throughput and download reliability compared to most centralized storage platforms, given their reduced potential for data bottlenecks or operational failures to interfere with data transfer operations. This is important when uploading or downloading large files and multi-file batch processing applications such as back-up storage drives. In this case the user does not typically mind waiting tens of seconds to initiate an upload or download process that may take tens of minutes or more to complete. Moreover, decentralized storage architectures can be designed to impart a high level of file security to the stored data. However, the large access latencies characteristic of

decentralized blockchain based platforms (typically 10-20 seconds or more) make them highly unsuitable for most individual online file management, sharing and editing applications. Furthermore, most enterprises require seamless fast management of all file storage, editing and sharing applications between hundreds or thousands of employees, clients and customers. Consequently, using a blockchain based storage platform in an enterprise environment becomes impractical and cumbersome for the user.

Figure 2b (right) plots the measured access latencies of various commercial storage platforms versus node number[6]. Blockchain platforms require verification of all actions via multiple confirming iterations of a consensus driven engine and involve a large number of participating storage nodes (ie: 20 – 10,000 nodes). Moreover, as user adoption of a blockchain platform scales to very large numbers the access latency can also increase significantly. Throughput generally scales with size much better than access latency in a decentralized system. The more nodes used to drive the consensus engine in a blockchain platform, the larger the access latency exhibited by the platform. Widely adopted blockchain platforms such as transaction focused Bitcoin and Ethereum currently exhibit access latencies ranging from several minutes to several hours (ie: 200 – 5000 seconds). This is a direct consequence of the large number of consensus nodes used in these platforms (ie: 8,000 – 20,000 nodes). Nonetheless, while these very large latencies are highly unsuitable for most online applications such as file storage and sharing, they are still relatively small compared to transaction times of competitive financial technologies such as wire transfers between centralized banks. Blockchains that use smaller node numbers such as Sia and Filecoin (ie: 20 – 50 nodes) exhibit proportionally smaller latency times (ie: 10 – 100 seconds). However, the iterative consensus driven nature of these blockchain platforms adds additional latency. These platforms are well suited for large file storage applications such as back-up network storage and immutable database ledgers. Although these platforms exhibit a reduced degree of latency, they are still too slow for real-time online applications used by enterprises such file management, sharing and editing.

**Figure 2b: Latency vs Node Number**




Also shown in Figure 2b is the typical latency for conventional centralized platforms such as Google Drive and Amazon S3 (ie: single node). With access latencies of the order of 100 milliseconds

these dedicated single vendor cloud platforms are ideal for user-friendly file management and editing applications. However, these centralized storage platforms are also characterized by large attack vectors and poor security profiles. Ideally, a decentralized platform with high scalable throughput, reduced attack surface and low access latency is desired for most enterprise-class file storage applications. By comparing Figure 2a (Attack Surface versus Node Number) with Figure 2b (Latency versus Node Number) we can identify that the sweet spot for compromise between minimal attack surface and low latency is for a node number around 5 storage nodes (labelled *Sweet Spot in Figure 2b). For this relatively low order of decentralization the attack surface is still reduced by over 90% while the latency is also very low (ie: 200-300 msec). Hence a 5-node storage platform appears an ideal compromise between performance and security for enterprise-class applications. However, consensus driven blockchain platforms typically require at least 20 nodes to function effectively and hence a blockchain design is not appropriate for this relatively low degree of decentralization. The most practical architecture for a 5-node online storage platform utilizes dedicated connections to multiple 3rd party cloud vendors such as Google and Amazon.

## 2(c). Cost Structures for Enterprise Security and Storage Applications

We have already discussed in Section 2(b) how blockchain based storage platforms such as Sia and Filecoin are not suitable for real-time file management and editing applications because of their large access latencies. Consequently, these blockchain storage platforms are better suited for very large file sizes and batch storage applications such as data back-up and restoration. However, even for such large file size applications, these blockchain storage platforms are primarily only suited for consumer markets because of cost structure issues. Although blockchain technologies can be disruptive to many markets this generally requires large costs savings for the customer. However, online storage pricing from conventional cloud storage providers is already at a very low commodity level (ie: around $5 per TB / user / month). Blockchain platforms such as Sia offer cheaper storage pricing that is typically 40-80% of conventional cloud storage providers (ie: around $2 - $4 per TB / user / month). While migrating online file storage to a more secure, lower cost blockchain based platform might hold appeal for the individual consumer, this option holds very little appeal for the enterprise customer.

Reducing online storage costs is not the decisive factor for an enterprise because storage costs are relatively insignificant compared to the cost of deploying a complete security solution for file storage. It is important to note that while decentralized platforms offer greater protection against security breaches, this is only for protection against external threats and operational failures. Decentralization by itself does not offer any added security against internal, viral and surveillance threats. Of prime importance to all large enterprises and organizations is the ever-present security threat from internal sources (ie: employees) which is not typically an issue for individual consumers. To mitigate against internal, viral and

surveillance threats enterprises typically spend another $40 - $80 / user / month. The benefit for an enterprise saving only $1 - $3 / user / month for migrating to a blockchain storage platform is irrelevant when also considering the major cost of a complete security solution and the increased degree of latency. Hence blockchain technology has little potential to disrupt enterprise storage markets because of cost structure and latency issues. Nonetheless blockchain technology holds great potential for the disruption of enterprise security markets as security products are the primary cost factor when deploying enterprise storage. There exists significant demand for a decentralized storage solution for enterprise customers that exhibits low access latency, broad security protection and reduced operational costs.

## 3. CRYPTYK Platform Architecture

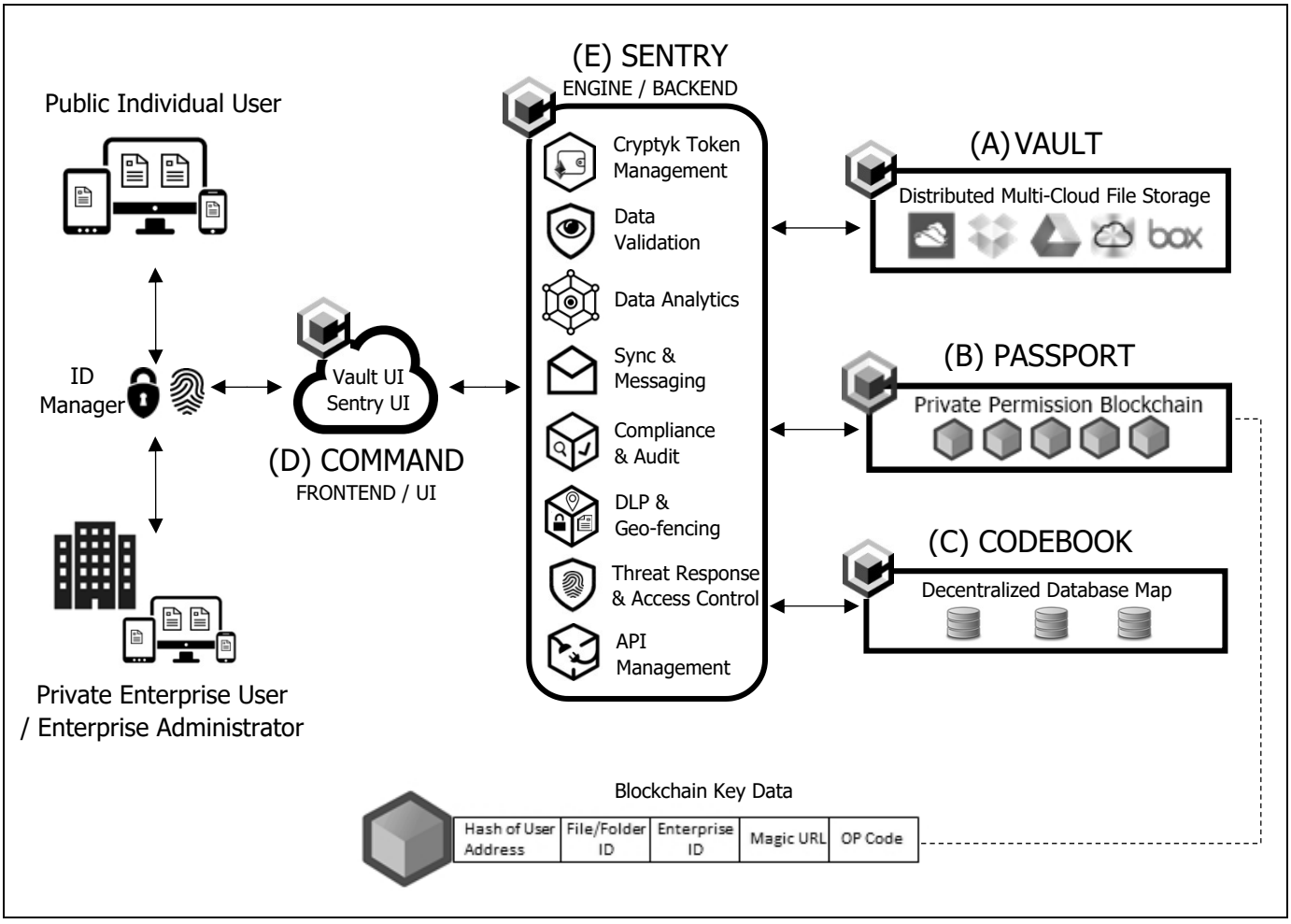
Low cost cloud storage services for data-at-rest applications are a fundamental weakness for all conventional security solutions that are complex and expensive to deploy. Building a complete enterprise-class security solution must also incorporate cloud storage as a fundamental building block to ensure an optimal security profile. The design philosophy that underpins the hybrid CRYPTYK architecture is based on optimizing specific characteristics of three different decentralized platforms to meet the varying multitude of critical performance requirements for both enterprise security and storage applications. Not every decentralized platform is ideal for every online application and it requires the integration of three different but complimentary platforms to meet the broad performance and usability demands for a complete enterprise-class security and storage solution. Cryptyk digital tokens or CTKs are an essential ingredient that powers the entire CRYPTYK platform architecture by:

- Enabling the three different decentralized storage platforms (VAULT, PASSPORT and CODEBOOK) to operate with each other and provide multiple layers of security,
- Allowing enterprise customers and individual users to purchase a complete range of security and storage services,
- Providing incentives for enterprise customers to initially trial and deploy security and storage services,
- Providing incentives for open source developers and alliance partners to support the CTK ecosystem by developing an expanding range of compatible API and plug-in products, and
- Providing incentives for ecosystem participants and crypto-currency miners to preferentially process CTK Proof of Security (Ps) calculations that powers the private blockchain platform PASSPORT.

The CRYPTYK solution does not attempt to disrupt the existing cloud storage market by displacing large entrenched players that already provide reliable storage services at very low commodity level prices. Instead it combines a more secure decentralized multi-cloud storage platform (that leverages existing storage services from major cloud providers) with two decentralized blockchain security platforms that verify, record and manage user access and file sharing for individuals and enterprises. Consequently, the CRYPTYK solution disrupts the much larger enterprise security market by providing a more secure and cost-effective product bundle that includes both enterprise security and cloud storage services. Nonetheless the CRYPTYK solution offers a cost competitive solution for cloud storage alone.

Products and services built on the CRYPTYK platform architecture have the potential to displace a variety of more expensive products and services from existing vendors in the enterprise security market such as CASB, CSG, DLP, Firewall and Threat Monitoring products. The benefits for both enterprise and individual customers include (i) dramatic improvements in security profiles, (ii) simpler trial and deployment of products via a single product solution, and (iii) lower total operational costs for online security and storage.

**Figure 3: High-level overview of CRYPTYK architecture**



A high-level overview of the CRYPTYK platform architecture is shown above in Figure 3. The CRYPTYK platform comprises six key components, namely:

(A) VAULT: Distributed, User-Encrypted, Multi-Cloud File Storage and Sharing Platform.
(B) PASSPORT: Private Permission Blockchain Platform for user access / file sharing ledger.
(C) CODEBOOK: Decentralized Database Map for internal data and file encryption key storage.
(D) COMMAND: Cloud-based or Client-based user interface and frontend control panel / UX.
(E) SENTRY: Core engine / backend integrates all other components & manages all operations.

All individual and enterprise users require a conventional User Identity Manager product with Multi-Factor Authentication (MFA) such as Google Authenticator or LastPass to access the CRYPTYK platform via either a cloud-based frontend user interface or a local client-based program. Public individual users receive a free version of the passively secure VAULT file storage platform with limited security management features and file storage space (eg: 1GB of storage). While the VAULT platform is passively immune to external, viral and operational threats it offers no protection against internal or surveillance threats. However, users can also choose to purchase additional security management features via the SENTRY security engine that protects against surveillance threats and the PASSPORT blockchain network that provides a powerful security tool to protect against internal threats (again not an issue for most public users). Users can also upgrade to larger file storage capacity on the VAULT platform (eg: 1TB of storage). The COMMAND user interface for individual users has policy settings configured for the high personal privacy but limited discovery appropriate for members of the general public. Nonetheless if files are shared with an individual user the original author or sharer of the file can set user access and file permissions for each individual file within a shared group of users. The CODEBOOK database map platform is an internal database map for the SENTRY engine and consequently has no direct interaction with the user apart from account back-up services. Similarly, the PASSPORT blockchain is an internal immutable ledger that operates behind the scenes oblivious to the public user. The CRYPTYK storage and security product bundle is both superior in security and lower in cost than conventional security and storage solutions for individual public customers.

Enterprise customers first trial and then can purchase the CRYPTYK hybrid platform with full storage capabilities (eg: 1TB of storage / user) including the PASSPORT private blockchain security platform and SENTRY security engine. Each enterprise customer is issued a unique enterprise ID that is built into the PASSPORT blockchain key data for all enterprise employees. Each individual user within the enterprise is also issued a unique user ID that also forms part of their specific blockchain key data. All employees or members of an enterprise use a version of the COMMAND user interface that is configured

by the enterprise for reduced privacy settings compared to individual public users. This effectively means that the private blockchain platform PASSPORT is opaque in nature and customizable via the COMMAND interface settings for policies and permissions. Cryptyk Inc. will design, implement and deploy a role-based access control system with a unique permissions architecture for the COMMAND interface. Authorized network administrators for enterprise customers receive an administration version of the COMMAND interface that allows them complete visibility of PASSPORT blockchain data, management of enterprise user access, control of file access permissions, setting of enterprise policies, tracking of all file sharing transactions and granular selection of security configurations.

Cryptyk Inc. will also design, implement and deploy a standardized API format that specifies and enforces various security profiles and configurations. It is envisaged that future open source API and plug-in development will produce industry specific bridges that allow application interfaces between internal users of two or more different enterprises with different enterprise ID's. Most importantly for viral adoption, whenever an employee of an enterprise shares a file with a customer or individual member of the public outside of the enterprise, the customer or public individual receives the feature-limited free version of the VAULT product, some of who will ultimately upgrade to the paid product bundle with increased storage and superior security features. Consequently, targeting the complete CRYTYK product bundle at enterprise customers will ultimately produce adoption of both storage and security products by public individuals via the network effect of file sharing interactions with external customers or clients. The complete enterprise-class storage and security product bundle is both superior in security profile and dramatically lower in cost than conventional security and storage solutions for enterprise.

## 4. CRYPTYK Platform Components

We will now discuss the specific design parameters, security capabilities and product features of the six critical components that combine to make up the CRYPTYK platform architecture.

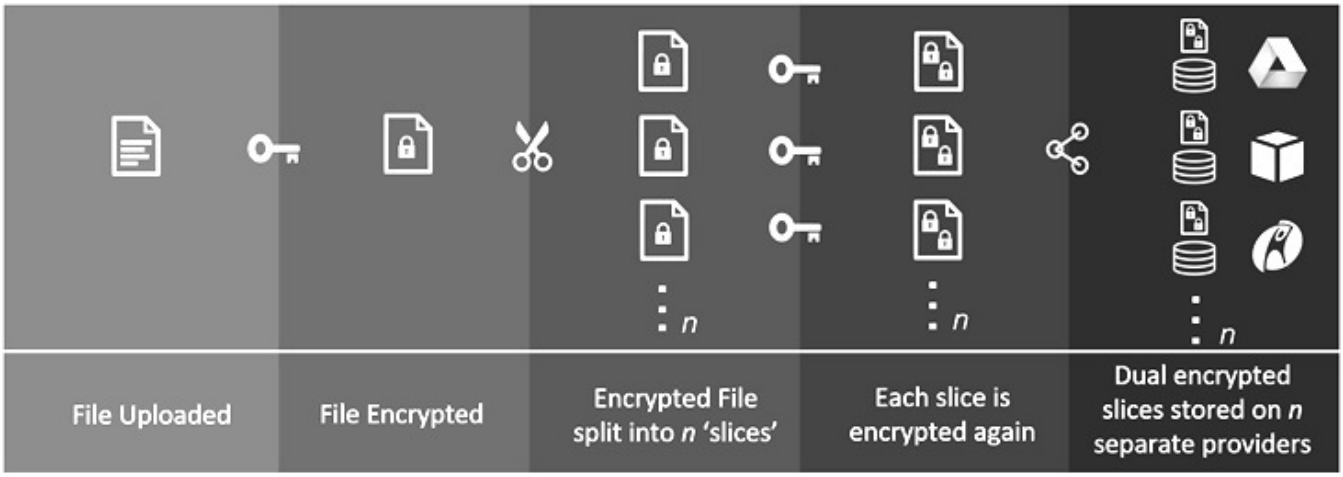
### 4(a). Distributed Multi-Cloud File Storage and Sharing Platform (VAULT)

The underlying foundation of the CRYPTYK ecosystem is the Distributed, User-Encrypted, Multi-Cloud File Storage and Sharing Platform called VAULT. The design of VAULT utilizes a limited degree of decentralization through multiple dedicated storage nodes (ie: 5 – 10 nodes) supplied by major cloud storage providers such as Google Drive, Amazon S3, Apple iCloud, Microsoft Azure, Box, Dropbox and Rackspace. The three critical design features of VAULT are that (1) it divides each and every file into multiple encrypted file portions that are stored separately on independent cloud storage providers, and (2) it stores the encryption keys that unlock access to each individual file portion on the users own local

fingerprinted smart device and the offline back-up portion of the CODEBOOK decentralized database map, and (3) it reduces over 90% of the potential attack surface while only adding 50% - 100% to the access latency of a single cloud storage provider (ie: 150-200msec latency compared to 100msec latency from a single vendor). Consequently, external security breaches of any individual cloud storage provider can only provide access to a small useless portion of any stored file, even if multiple encryption layers are broken. The theft of data from a single user requires both physical access to that internal user's personal device and their CRYPTYK user account. Even in these cases only files approved for that specific user can be accessed. Consequently, large scale hacking of multiple users is simply not practical nor viable.

Figure 4 below details the preferred splicing and encryption method for a distributed multi-cloud file storage platform. Each individual file that is uploaded to the VAULT platform is first encrypted and then sliced into *n* different file portions or slices. Each of these *n* slices is then encrypted again and stored separately on *n* third party cloud storage providers (such as Amazon S3, Google Drive or Rackspace). Each file is stored in a decentralized format across *n* independent storage providers, using *n*+1 encryption keys that can be stored on the user's personal device or a secure immutable blockchain network. If the user shares access of this file with another individual then that individual receives a free version of VAULT with a user account that has permission to access to the six encryption keys for the shared file. Hence the platform operates effectively as a highly secure file storage and file sharing service.

**Figure 4: VAULT File slicing and encryption method**




The VAULT platform removes significant risk from using 3rd party cloud storage vendors and takes the profit out of external breaches by criminal syndicates. Furthermore, if viral software is uploaded then the virus or malware file only exists as multiple separately partitioned and encrypted file portions that cannot interact with each other to form an executable program. Consequently, this decentralized design is also passively immune to viral security threats and does not rely on continual anti-virus scanning

software that adds to access latency and requires frequent updating. The encryption and storage algorithm employs a redundant storage format (similar to RAID architecture) that also ensures 24/7/365 operational reliability even if any single cloud storage provider experiences an operational failure. This can be achieved by adding a layer of staggered redundancy to the file portions across multiple storage nodes in a similar manner to conventional RAID storage architecture[7]. Hence the VAULT platform is passively immune to three out of the five main security threats to enterprise (ie: external, viral and operational) and does not require regular product updates to ensure ongoing data protection. Nonetheless the distributed file storage platform is still vulnerable to security breaches from internal sources and surveillance of communications between individuals. Both internal and surveillance threats are major concerns to all businesses, enterprises and organizations. However, internal threats are not usually of concern to individual public users and surveillance / data intercept threats remain their prime vulnerability.

## 4(b). Private Permission Blockchain Security Platform (PASSPORT)

The purpose of the PASSPORT private blockchain security platform is (a) to provide a permanent, immutable and auditable record of all enterprise ID, user ID, file / folder ID, user access sessions, magic URL's and operational history of the CRYPTYK platform by all users, and (b) to provide customizable permissioned access (with varying degrees of opacity) to public individual users, private enterprise users and enterprise administrators of all user access and file transaction information including file creation, deletion, editing, reviewing, updating and sharing. The PASSPORT platform will preferably be built from the ground up as a new blockchain architecture and protocol unique to the Cryptyk platform requirements. However, it may also be easily built on top of third party blockchain architecture such as Ethereum[8] or Hyperledger[9] configured in private blockchain mode. The latter option is no doubt the easiest and most cost-effective solution for deployment. However current versions of leading third party blockchains are non-ideal and a suitably secure and scalable third-party option is not yet known at this time. Hence Cryptyk will likely develop or co-develop the most secure, customizable and scalable option for its blockchain architecture that suits the specific needs of its hybrid decentralized platform.

The customizable permissioned blockchain architecture provides the ability for enterprise administrators to track, analyze and audit all enterprise user behavior and all file transfers owned by the enterprise (ie: all employee files). For an approved enterprise administrator, this granular visibility goes beyond just tracking enterprise users and extends to tracking individual public users who have been permitted access to files owned or created by an enterprise employee. It also provides enterprise users, employees and individual public users the ability to track the file sharing history and user access to personal files owned or created by themselves. The individual user can set the level of security access to an individual file dependent on the nature of the person that they are sharing with. Such a platform design

allows the authorized creator or owner of an individual file to securely share, monitor and track a files access history with a wide range of customizable security features and permission levels.

Design of a private permissioned blockchain security platform that caters for both individual public users and private enterprise administrators must accommodate a wide range of possible variables set on a very granular level. The customizable opaque nature of the PASSPORT blockchain design combined with the granular nature of the VAULT file storage platform offers finely tuned control over data visibility and data privacy for individual file access. PASSPORT provides both individuals and enterprises with a permanent record of all file transactions and user activity in an analogous manner to international passports and visas providing a record of personal travel activity between different nations. Consequently, this blockchain design with customizable discovery properties makes an ideal security architecture for analyzing, managing and protecting against internal security threats to an enterprise. When combined with the passive security features of the VAULT file storage platform this blockchain / multi-cloud hybrid solution protects against all external, viral, operational and internal security threats.

From a blockchain design perspective, the PASSPORT platform utilizes a novel form of consensus driven verification called Proof of Security verification. The blockchain consensus settings and verified blockchain results are managed and audited by the SENTRY core engine and back-end (see Section 4e). We define Proof of Security (Ps) as a function of Proof of Integrity (Pi), Proof of Confidentiality (Pc), Proof of Access (Pa), Proof of Posture (Pp) and Proof of Compliance (Pc) such that

$$Ps = F\ \{f(Pi), f(Pc), f(Pa), f(Pp), f(Pc)\}$$

The five verification proofs that comprise Proof of Security for a file or user event are described as:

- Proof of Integrity is verification of the integrity of the file and proof that it is not a malicious application or viral code (note this does not decrypt the file).
- Proof of Confidentiality is verification that the file is secure against an attacker's attempt to copy or decrypt the file.
- Proof of Access is a verification function of role based access control (RBAC), geo-location, file level permissions and multi-factor authorization (MFA).
- Proof of Posture is a verification function of user device fingerprint score, security posture of the device and threat protection analysis.
- Proof of Compliance is a verification function of compliancy requirements, regulation requirements, legal requirements, organization policies, procedures and objectives.

CRYPTYK participants and CTK miners (or brokers) get rewarded in CTK tokens for correctly verifying the Proof of Security for any particular file transaction or user action via the decentralized consensus-driven blockchain engine.

## 4(c). Decentralized Database Map (CODEBOOK)

The purpose of the CODEBOOK decentralized database map is to (a) securely store an offline back-up copy all file encryption keys (6 keys for each file stored in VAULT) for all individual public and enterprise users in case of loss or damage of the user's smart device or personal computer, (b) to securely store online all policy information, audit data, user logs, reports, transaction data and compliance data. Although there exists a plethora of conventional options for database maps such as centralized relational databases, the preferred solution should utilize a more secure decentralized database ledger platform such as BigchainDB[10], Cockroach DB[11] or Hashgraph[12]. For both security and customizability reasons these database platforms are well suited for integration with a distributed file system manager such as the VAULT platform and a private permissioned blockchain ledger such as the PASSPORT platform. The preferred download configuration for the offline database map of all file encryption keys should use a one-directional database transfer mechanism (eg: photonic diode) with an online file cache to the off-line server. Access to back-up encryption keys for customers with lost or corrupted devices is provided by providing an online link to a time-limited copy of all encryption keys authorized for the specific user.

## 4(d). User Control Interface / Frontend (COMMAND)

The purpose of the COMMAND frontend user control interface is (a) to provide all users a highly customizable and easy-to-use interface to manage all file storage, sharing and security activities utilizing the SENTRY backend engine and three decentralized storage platforms, and (b) to provide a product purchasing interface for payment of various security and storage products in both fiat currency (ie: USD) and Cryptyk Tokens (ie: CTKs). Depending on the solution purchased by each customer and type of user (public individual, enterprise user or enterprise administrator) the various security, privacy, visibility and administration features are either enabled or disabled for each user. The user control interface may be either a cloud-based or local client-based user interface for access to the rest of the CRYPTYK. It is anticipated that most public individual users and enterprise users will choose to use the cloud-based interface out of simplicity, device mobility and ease of data synchronization. However, enterprise administrators may prefer a local client based interface because of organizational protocols and procedures. Access to the frontend requires a MFA application developed by Cryptyk or third party MFA application such as Google Authenticator or LastPass. At its essence, the COMMAND frontend platform is a secure window or pane of glass that allows granular observation and control of all data stored on the

hybrid CRYPTYK platform. It provides this function with varying degrees of data transparency and privacy dependent on the user type and enterprise policy setting for a particular file, folder or user action. From a customer point of view, the COMMAND frontend appears as a two complimentary user interfaces that allows management of the VAULT file storage platform and the SENTRY security engine. The two-for-one VAULT + SENTRY product bundle forms a complete cloud storage and security solution.

## 4(e). Security Engine and Backend (SENTRY)

Cryptyk will design, develop and deploy the SENTRY security engine and backend platform to (a) provide the data management, logic processing, policy enforcement, data analysis and encryption engine that powers the flow of CTK tokens to token miners in return for enterprise security and storage services, (b) provide the central interconnect between the COMMAND user interface and the three decentralized storage platform components VAULT (for file storage), PASSPORT (for user / file activity log) and CODEBOOK (for file key back-up / database map), (c) manage the consensus driven Proof of Security protocol settings and results and (d) to provide responsible management of the CTK ecosystem for the incentivization of all CRYPTYK platform participants including enterprise customers, enterprise users, individual public users, customer alliance partners, strategic development partners, open-source developers, token sale investors and CTK miners.

SENTRY manages all encryption, data validation, data analytics, synchronization, messaging, compliance, auditing, policy enforcement, data leak prevention, geo-fencing and threat analysis functions. Consequently, the backend acts as an additional security layer that surrounds all other platform components and protects all users against surveillance threats when sending emails, chats or transactions. It also manages the interaction with APIs developed by 3rd party app developers, strategic development partners, customer alliance partners and Cryptyk Inc. Most importantly the backend also manages all CTK token ecosystem activities including customer trials, customer purchases, mining payments, developer payments, strategic partner payments and token exchange with both digital currencies (such as Ethereum and Bitcoin) and fiat currency (such as US dollar and Euros). The fundamental purpose of the CTK ecosystem structure is to incentivize and grow enterprise adoption of the CTYPTYK platform

When purchasing the complete hybrid CRYPTYK platform (containing the VAULT, SENTRY and PASSPORT storage components) enterprise customers first trial the platform and can then choose to purchase various features of a customized security and storage bundle for between $20 and $30 / user / month for 1TB of user account storage. This is anticipated to be less than half of the total security and storage costs for comparable conventional solutions from multiple storage and security vendors. Moreover, it is a much more complete security solution for the enterprise customer with a vastly reduced

attack surface against all five major security threats. Compared to blockchain-only file storage platforms such as Sia and Filecoin, the CRYPTYK hybrid bundle offers dramatic improvements in security profile, access latency, platform usability, product features and cost structures.

### (4f) Additional Storage Configurations for Enterprise

While the primary storage configuration presented here for the VAULT platform utilizes multiple cloud storage nodes from multiple 3rd party cloud storage providers such as Amazon and Google, the unique distributed user-encrypted storage method can also be applied to other types of storage nodes for similar security benefits. Of particular importance is the case when the platform is configured to use multiple existing internal storage servers as storage nodes. While using storage servers owned by the same enterprise entity does not offer the same security level of the multi-cloud VAULT configuration where each storage node is completely independent of each other, this enterprise network configuration provides dramatically improved security over conventional enterprise server storage methods. An enterprise network VAULT platform deployed on an internal storage server network should exhibit improved access latency and throughput compared to the online multi-cloud configuration. Moreover, a multi-cloud VAULT platform can be easily integrated with an enterprise network VAULT platform to form a hybrid storage platform that enables easy migration of data between the internal enterprise and the cloud. Other storage configurations that use storage nodes across multiple enterprise networks in a federated alliance of businesses are also possible. Nonetheless the original multi-cloud VAULT configuration remains the most secure option (because of the independence of multiple cloud storage vendors), while also allowing great employee mobility and data accessibility. Regardless of whether cloud, hybrid, on-premise or federated storage configurations are implemented, the fundamental nature of the VAULT file storage platform remains. Specifically, the user-encrypted file-decentralized nature of the storage architecture means that VAULT storage configurations are passively immune to external, viral and operational threats.

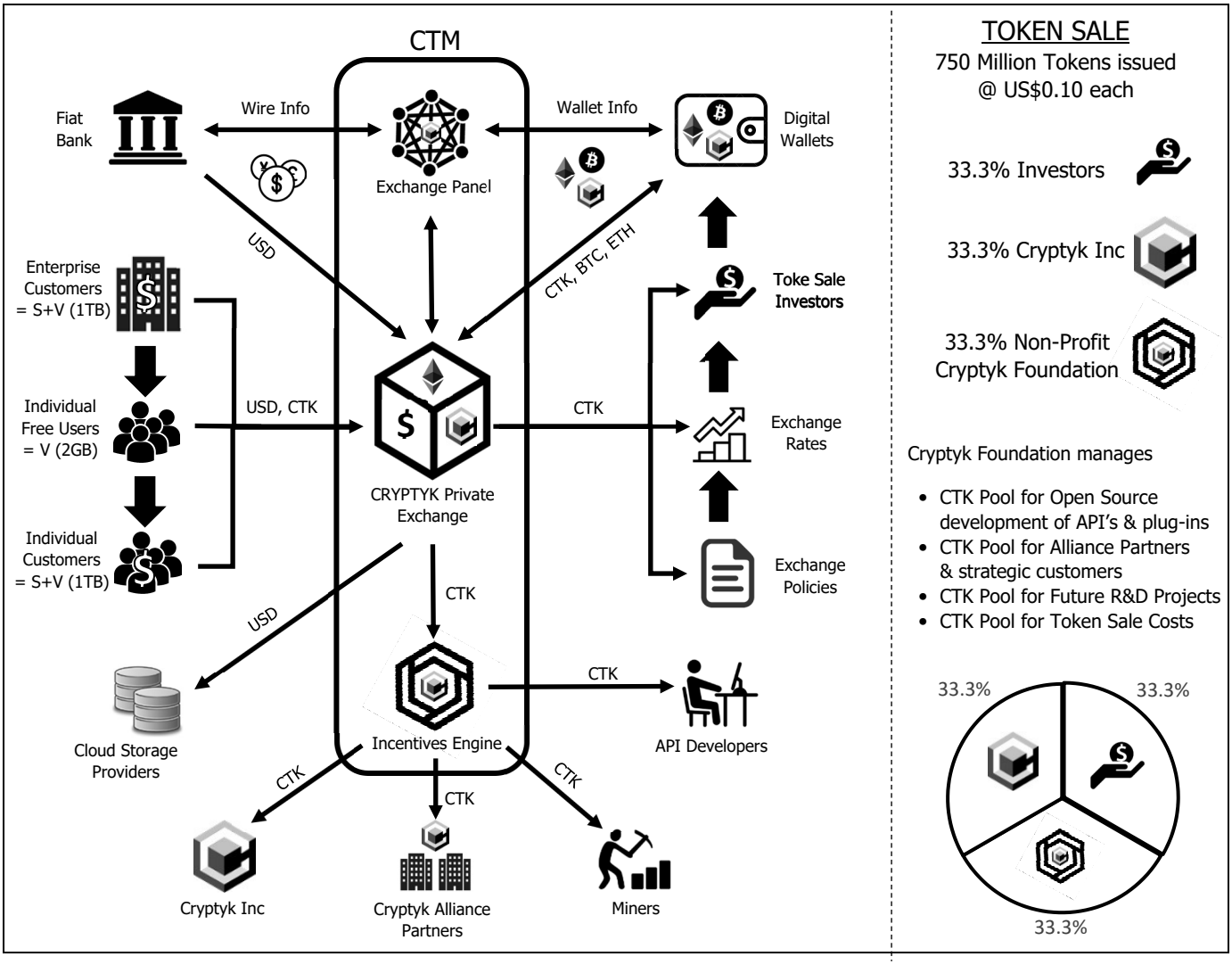
## (5). CRYPTYK Token Management

CRYPTYK digital tokens (ie: CTKs) are essential to power the CRYPTYK hybrid platform and allow each of the three decentralized platforms to communicate with each other to provide a complete, interoperable security and storage solution for the customer. Consequently, efficient management of the supply, demand and flow of CTKs is critical for the scalable, profitable growth of the entire ecosystem according to fundamental crypto-economic principles. To manage the digital token ecosystem the CRYPTYK Token Management (CTM) platform forms a component of the backend engine called

SENTRY as shown above in Figure 3. The detailed architecture of the CTM platform is shown below in Figure 5 and comprises 3 main components, namely:

- CRYPTYK Exchange Panel which interfaces with fiat currency banks (nominally in USD) digital currency wallets (in CTK, Bitcoin or Ethereum), and manages all transactions in CTK tokens, fiat currencies and digital currencies (fixed in USD).
- CRYPTYK Private Exchange which authorizes Cryptyk product activations, manages customer invoicing and payments, makes payments to cloud storage providers such as Amazon and Google (fixed in USD), and enables the interaction and flow of all CTK tokens, fiat currencies and digital currencies between all ecosystem participants.
- CRYPTYK Incentives Engine which receives profits in CTK from the CRYPTYK Private Exchange, shares profits in CTK between Cryptyk Inc. and CRYPTYK Miners, makes payments to open source developers for building APIs that interface with 3rd party software, and provides financial incentives to Strategic Alliance Partners to trial Cryptyk products.

**Figure 5: The Cryptyk Token Management (CTM) Platform**



Successful, scalable and profitable growth of the CRYPTYK platform over time requires optimization of the initial structure of the token sale offering with a fixed total number of CTKs to be created and then released appropriately over time according to the smart contract framework for the token sale. Investors in the token sale can purchase up to one third or 33.3% of a capped total of a total of 750 million CTKs created (ie: 250 million CTKs at an initial sale price around 10 cents each). Another 250 million or 33.3% of CTKs are reserved for the shareholders of Cryptyk Inc who can slowly exchange their equity for tokens over a two to four year vesting period (depending on whether they are founders, investors, advisors or employees). The remaining 250 million CTKs are reserved in a pool for distribution by a non-profit entity called the Cryptyk Foundation. The Cryptyk Foundation manages the rules and optimizes the settings for the Cryptyk incentives engine that shares profit from customer revenues between CTK miners and Cryptyk Inc. The Cryptyk Foundation also manages the reserved pool of 250 million CTK's for future rewards to open-source API developers, strategic alliance customers, future research and development projects and pays for the operational costs of the public token sale. This three-way token generation structure is intended to ensure the rapid trial and adoption of Cryptyk products by strategic alliance customers, and to encourage the open-source development of platform features by 3rd party API developers and strategic development partners.

The total number of tokens is forever limited to 750 million upon the initial token issue, and consequently the simple process of customer adoption will increase CTK demand assuming responsible governance and pragmatic token-economic strategies implemented by the Cryptyk Foundation. The fundamental purpose of the non-profit entity in the Cryptyk Foundation owning 33.3% of all issued tokens is to provide a publicly transparent method for the entire CTK community to become involved in the CRYPTYK project and regulate incentives and rewards. It is also intended to provide the appropriate degree of token scarcity and financial liquidity in the CTK marketplace that can only be increased through ongoing platform development and customer adoption. Ultimately this should ensure less volatility in the short-term CTK value and provide for significant long-term growth in CTK value based on platform adoption by enterprise customers.

The Cryptyk Foundation will authorize and distribute parcels of tokens to Alliance Customers and Strategic Development Partners to seed the market adoption of Cryptyk products, to seed the growth of an open source developer community and to fund future platform development projects. It will also fund all token sale costs and infrastructure set-up costs that may include payment for smart contract development, exchange listing, employee / team bonuses and incorporation and management costs. It is anticipated that the Cryptyk Foundation pool of 250 million tokens will be completely expended via sale

on listed exchanges within the 4 years of the initial token sale. Within that period all Cryptyk Foundation issued tokens should be circulating within the growing CTK investor, developer and customer communities.

The Cryptyk Foundation will grow the Cryptyk open source developer community on a pay-for-plug-in basis with CTK incentives for individual API developers and software coders. It will be responsible for reviewing the rules of the incentives engine and over-sight of the profit-sharing agreements between Cryptyk Inc, Cryptyk Foundation and CTK Miners (who may effectively be Ethereum miners if the platform is based on the Ethereum blockchain protocol). While Cryptyk Inc and CTK Miners share the majority of profits generated from product sales, the Cryptyk Foundation receives some small portion of profits from the incentives engine to ensure there will always be a sufficiently large pool of CTKs for distribution to all participants as the growth of the ecosystem scales. It is envisaged that the Cryptyk Foundation will be managed by a board of directors that include senior members of Cryptyk Inc, Alliance Customers and Open-Source Development Partners. The complete token management ecosystem is ideally suited to providing cost benefits for enterprise customers and positive token-flow for all non-customer participants. Scalable product adoption will directly translate to significant long-term growth in the token value for all owners of CTKs. Significant long-term growth in the CTK value benefits all investors, customers, developers, miners and alliance partners.

## (6). Crypto-Economics and Token Value Analysis

The CRYPTYK platform utilizes a viral crypto-economic model comprising two different but complimentary business models for decentralized network architectures. The primary benefits of using a decentralized multi-cloud platform for file storage and sharing are low access latency, minimal attack surface, large scalability, high data resiliency and commodity level pricing from large trusted cloud storage vendors. This multi-cloud file storage platform encourages viral adoption via file sharing between enterprise employees and their external customers and clients (which become either free or paid customers of Cryptyk Inc.). Importantly all file storage costs are fixed in local fiat currency such as USD or Euros.

The primary benefits of using a decentralized private blockchain platform for managing user access and file tracking / auditing activities are:

- Customizable permissioned access to a permanent immutable record of all user access and file sharing activities within an enterprise and between an enterprise and its customers,
- Reduced attack surface for managing all internal and surveillance security threats via a decentralized, scalable, immutable ledger database of all user access and file sharing events,

- Initial user base to stimulate the initial trial and adoption of Cryptyk products and services via a supportive community of Alliance Partners, Open Source Developers and CTK investors,
- Viral network effect that encourages the utility and exchange of CTK tokens for security and storage services more than it encourages speculative investment in CTK token value growth as listed on crypto-currency or token exchanges, and
- Inevitable long-term growth in CTK value with increasing customer adoption by enterprise customers, regardless of short term speculative fluctuations in CTK value from investors.

Critical to driving these benefits for the CTK ecosystem and all its participants is that all pricing for enterprise security and storage services offered by Cryptyk Inc. is fixed in fiat currency such as USD or Euros. Furthermore, customers may pay for security and storage services with either CTK's or with fiat currency. If the customer chooses to pay in fiat currency this is automatically converted into CTK's via the Exchange Panel of the Cryptyk Token Management platform. Consequently, paying for use of the CRYTPYK platform and its services in either CTK's or fiat currency increases the demand for tokens and in turn drives CTK value upwards. Moreover, this design also encourages the large pre-purchase of CTK tokens by customers to pay upfront for services over the long term.

For example, a customer may purchase say US$600,000 of CTK tokens for six months of security and storage services at US$100,000 per month. If the customer pre-purchases CTK's for these services and pays in CTK's on a monthly basis, the CTK token value may increase 2-3 times in value over the six-month period. As all pricing is fixed in USD this means that the monthly price in CTK's has decreased in value by 2-3 times. Consequently, pre-purchasing CTK tokens can mean an ever-diminishing cost for security and storage services over time (assuming an increase in token value due to growth in customer adoption). Very early stage customers such as Alliance partners may ultimately find themselves paying cents on the dollar for all their cloud storage and security services. Ultimately, the more utility in the token the more value for both customers and investors in terms of product pricing and CTK pricing.

One of the biggest problems with most crypto-currencies and digital token ecosystems is a lack of utility in the coin or token compared to its speculative use as an investment. Consequently, many crypto-currencies and digital tokens are now being classified by government regulatory organizations as securities instead of utility tokens or products for sale. For example, the leading crypto-currency bitcoin was developed as a replacement for credit and debit cards when purchasing retail products from merchants. Bitcoin reduces the cost of retail purchases by a factor of 5-6. Bitcoin transactions typically cost 0.5% - 0.6% per transaction instead of 2.5% - 3% per transaction as charged by banks and credit card companies. Unfortunately, the major problem with the bitcoin ecosystem is that merchants pay the existing credit card fees and not the customers. Merchants accepting bitcoin payments can save 2% in transaction fees and

choose to pass the savings onto the customer or not. However most retail merchants will only accept bitcoin if they observe enough customers demanding bitcoin payments. Given the price elasticity of retail products, a savings of a few percent in transaction costs is typically not enough to drive large scale merchant adoption. Hence a very large pool of potential customers wanting to pay in bitcoin must be built up first before bitcoin merchant adoption can become significant. Ignoring the usage of bitcoin for anonymity-driven applications such as gambling or payment for illegal products, the actual amount of bitcoin that is used by regular consumers to pay for legal retail products is extremely low[13] (of the order of a few percent of total bitcoin market capitalization). Consequently, bitcoin has a very low level of product utility for retail transactions compared to its primary usage as a speculative investment. Because the primary use of bitcoin is as an investment security, the lack of any adjustable liquidity process or product utility means that the price of bitcoin can fluctuate wildly according to investor sentiment.

In contrast the CRYPTYK ecosystem is designed for high product utility that drives inevitable price increases in CTK value over the long term, scaling directly with increasing customer adoption. Investors are investing in an enterprise product whose value is represented by the CTK value, and not in a company or asset security. Cryptyk Inc. is the only merchant that delivers this enterprise product and automatically accepts CTK tokens or USD. Consequently, no merchant adoption is required by the CTK ecosystem and customer adoption is driven purely by the massive demand in the enterprise market for more secure, simpler and cheaper cloud storage and security products. Moreover, the manual injection of CTK's into the ecosystem by the Cryptyk Foundation offers an efficient method for adjusting market liquidity in CTK's to counter speculative volatility.

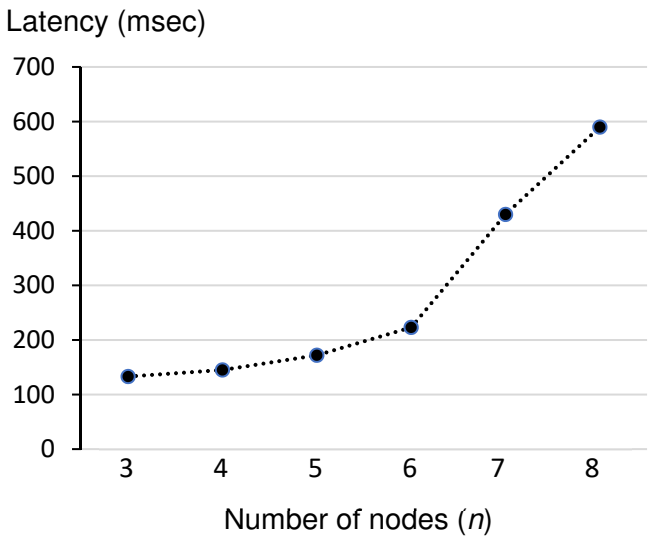
In contrast to bitcoin (that automatically has an ever-decreasing amount of coins released into the ecosystem subject to its mining protocol), the Cryptyk Foundation can manually increase or decrease the rate of release of tokens to customers, developers and miners dependent upon current market conditions and ecosystem valuation. This will act to counter or minimize spurious market fluctuations and large price spikes in CTK value as a result of speculative investors or bad actors. The non-profit Cryptyk Foundation will act to encourage customer adoption, grow the open source developer community, increase the long-term CTK value by orders of magnitude and stabilize any spurious fluctuations in market value.

Economic modelling of token usage suggests that the product utility of CTK tokens may ultimately grow to as much as 75% of the total CTK market capitalization in the long term, with the remaining 25% of tokens being used by investors for speculative purposes. Usage of the CRYPTYK platform by the entire CTK community (including customers, developers and investors), will ultimately be responsible for driving stable long-term growth in CTK value. By any reasonable assessment the CTK token can be defined as a true utility token (or product for sale) instead of as an investment security or crypto-currency.

## (7). Experimental Results

A prototype version of the CRYPTYK hybrid platform and ecosystem with simplified UI has been built by Cryptyk Inc and tested by over 40 invited cyber-security professionals over a test evaluation period of 3 months. The integrity of the platforms multi-faceted security profile was successfully verified as it proved immune to all implemented attack methods from a variety of different sources. Dramatic reductions in the attack surface for external, viral, internal and surveillance security threats have been successfully observed. Furthermore, the access latency for file upload operations was measured and analyzed for a range of node numbers (n = 3, 4, 5, 6, 7 and 8). Figure 6 shows the measured average access latency versus node number for a statistical sample of 5 uploads for each node configuration. Sub-second latencies increasing from 130msec to 590msec were observed for a node number ranging from 3 to 8. This is comparable to the 50-200msec latencies observed with single node cloud storage providers. While tolerable latencies have been achieved for even 8 nodes the ideal sweet spot for low access latency and reduced attack surface is observed to be either 5 or 6 storage nodes.

**Figure 6: Measured Latency vs Node Number**




## (8). Conclusions

A hybrid decentralized architecture for enterprise security and storage has been designed and described in detail. A simplified prototype version of the CRYPTYK platform with limited user interface features has been built and tested for security performance and access latency behavior. Dramatic improvements in security profile and significant reductions in attack surfaces have been observed for the hybrid decentralized platform when compared with conventional centralized security and storage solutions. The platform also has exhibited low sub-second latencies for configurations that use 3 to 8 storage nodes. This is considerably more usable than the 10-20 second latencies of other blockchain storage platforms such as Sia and Filecoin (only suitable for long duration back-up applications) and enables real-time enterprise cloud applications such as secure file sharing, live editing and chat. The CRYPTYK ecosystem also benefits from the viral network effect that occurs through token exchange and

file sharing activities. Consequently, the hybrid architecture exhibits the security, performance, latency usability and cost-efficiency requirements for enterprise-class security and storage applications.

A token management ecosystem and token economy infrastructure has also been proposed that offers ever-increasing incentives over time to enterprise customers, individual consumers, digital currency miners, open-source developers, strategic alliance partners, token sale investors and Cryptyk shareholders. The financial viability of the architecture is underpinned by the common alignment of all participant incentives for increased CTK payments and usage which will result in increased CTK value. The more customers that adopt Cryptyk products the more the CTK token will rise in scarcity and value. A complete fully featured hybrid platform that uses 5 – 6 cloud storage nodes will make the ideal security and storage solution for all small business and large enterprise. It will also provide huge financial opportunity for CTK investors, miners, vendors, alliance partners and open source developers. The CRYPTYK platform architecture and token ecosystem promises a truly complete, scalable and cost-effective solution that solves the critical security and storage problems for tomorrows businesses, enterprises and large organizations. The next step in the CRYTPYK project is to launch a token sale to investors for one third of 750 million generated tokens at an initially publicly traded price of 10 cents. Successful execution of a phased token sale launch will provide around $20 million for product development and initially create a $75 million ecosystem with the potential for growth into a multi-billion ecosystem via enterprise adoption.

## (9). References


1. Forbes Online Magazine (www.forbes.com) article titled “Cyber-crime costs projected to reach $2 Trillion by 2019”, Steve Morgan (Jan 17, 2016).

2. Markets and Markets research analyst report (www.marketsandmarkets.com) titled “Cyber-security Market by Solution, Service, Security Type, Deployment Mode, Organization Size, Vertical, and Region - Global Forecast to 2022” (July, 2017).

3. Published pricing data from CASB providers Skyhigh Networks, Bitglass and Cloudskope.

4. “Sia: Simple Decentralized Storage”, David Vorick and Luke Champine (Nov 29, 2014).

5. “Filecoin: A Decentralized Storage Network”, Protocol Labs (Aug 14, 2017).

6. Published access latency data from Sia, Filecoin, Ethereum, Bitcoin, Litecoin, Ripple, Hyperledger, Maidsafe, Google, Rackspace and Amazon.

7. “A Tutorial on RAID storage systems”, Sameshan Perumal and Pieter Kritzinger (May 6, 2004).

8. “Ethereum White Paper: A Next Generation Smart Contract and Decentralized Application Program”, Vitalik Buderin (January, 2014).

9. Hyperledger Project, www.hyperledger.org, Open source development project managed by the Linux Foundation, (December, 2015)

10. “BigchainDB: A Scalable Decentralized Database”, Trent McConaghy, Rudolph Marques, Andreas Muller, Dimitri De Jonghe, Troy McConaghy, Greg McMullen, Ryan Henderson, Sylvian Bellemare and Alberto Granzotto, (February, 2016)

11. CockroachDB design document, github.com/cockroachdb/cockroach/blob/master/docs/design.md Spencer Gimball, (February 2014)

12. “The Swirlds Hashgraph Consensus Algorithm: Fair, Fast, Byzantine Fault Tolerance”, Leemon Baird, (May 31, 2016).

13. “Bitcoin – Statistics and Facts”, Statistica, www.statista.com/topics/2308/bitcoin/ (October 2016).