1. P

Ý | F7 ý I 3 ÿ 7;Ñ 3 >ç wb

S# ã :É ™ XÀ à ³ ¢ Ø ™ Ž Â xR Ý $ç

À *ï× = Ð | FI S# ¯ƒ :Ñ

a ÿ à ÿD I7 Ò I2¿ ¹ Ô : zE, wb À à W

: þ aI S# Ñ Ý ýý I2Þ À– >b þ $÷– m

: Â ± Ô ™ Ø ÿ 7;Ñ :I R n7 ¢ ú >z

(TBü¡5-10ØW/)5ÿÀ, Ý‰ÿd ŠD Þ>z ²

(TBü ¡40-80ØW/)> ×ã à ÿ ‰ Ý R ÿÞ

ã S× Ø ðÞ y Á. Ža ‰ Ą 1LÞ I Ð >–3 Ñ

À Þ y Á. Ža ‰ ¶I R™ À Þ SÝ xØ ™ Ý ‰

Ý ‰ Ø $ Ł û SÑ, ySxK $ ÍÑ ã.. &@I Ñ

nÄ }Z ÿ 7;Ñ ¹> $ý Õ jIŠ ~ Ý ÿÀ wbà

}Z ¾ %à< jñ

Ý ÿ 7;Ñ Â Ý ‰ ý Ø K ƒ (á û S× Ž Ù

ŞÀ D“Þ ™ Ø ,.. ‡JÀ S# }Z ÿ 7;Ñ ¹× Ž

Iá ‰ zÀ Þ ‰ ç Þ Þ ™ Ø Ñ ¨

D Ý I 3 ú (dú û S# ;× Ý Ñ à ½ >Ñ ±

%8 uã S#

z5ÿ$–äÏçÒ û$

Ä c, ¯ Ò a–M7 Ø Ä$ ×

Ô–$–Âb z

E87Ò r$

E&0ß?@WNBOJOUIFNJEEMF z

I Ä Ñ à Ç Ý î–M7 Ø I FI X à H

WáS#

r ÿ 7;Ñ ÿ = ÿ à W/Ò }Ø }äBÞ

Ø ÿ }Ø W(CASB) ÿ %ÿ I(CSG)

Kbÿà á ä×KrW$8mÿ W}Ô L•

,3Þ,yÑSÿ

ŽVÒ(8K Ø)$ÿ(³

h ÿ LÂà Ø Ñam ÿ X2

Ôm Ì

· 위험한 블랙리스트 바이러스, 맬웨어 및 랜섬웨어를 검사하는 바이러스 백신 및 스파이웨어 소프트웨어

· 공용 / 개인 키와 함께 암호화 데이터 인코딩 알고리즘을 사용하여 저장된 데이터 및 이동되는 데이터 자산을 보호 및 감사하는 암호화 및 토큰화 도구.

클라우드 응용 프로그램을 위한 완벽한 기업용 보안 솔루션의 총 비용은 일반적으로사용자당 월 40~80 달러이며, 이는 클라우드 도입 계획을 결정하는 주요 비용 요소입니다. 그럼에도 불구하고, 이러한 기존 클라우드 보안 솔루션을 채택하는 대부분의 대기업들은 여전히 매년 보안 침해로 인해 상당한 손실을 입게 될 것입니다.

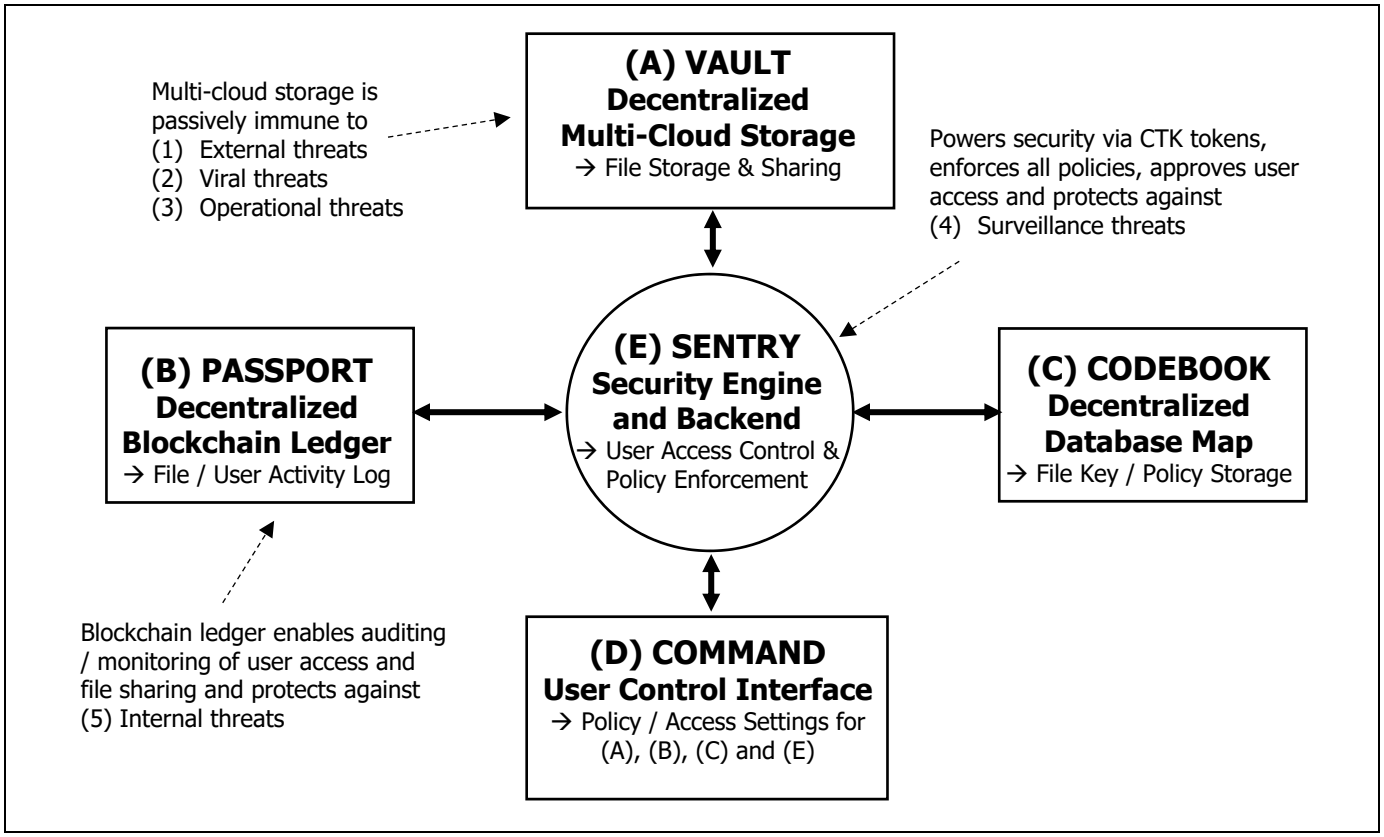
기존의 중앙 집중식 기업 보안 및 저장 기술과 달리, 여기에 제시된 CRYPTYK 플랫폼은 데이터 저장, 데이터 관리, 파일 공유, 파일 편집, 사용자 접속 및 이메일 및 데이터규정 준수에 대한 매우 안전하고 확장 가능한 제어를 위해 설계된 분산형 데이터 관리 아키텍처를 설명합니다. Sia와 Filecoin과 같은 블록체인 기술에 기반한 다른 분산형 파일 저장 플랫폼이 있지만, 여기에 설명된 하이브리드 CRYPTYK 플랫폼은 블록체인 전용 저장 기술의 고유 지연 문제를 겪지 않습니다. 기존 블록체인 저장 기술은 일반적으로 10~20초 이상, 최대 몇분 이상의 큰 접속 대기 시간을 보여 줍니다. 따라서 실시간 파일 관리, 사용 데이터 및 이동 데이터 응용 프로그램이 다중 사용자 기업 환경에서는 너무 느리고 사용할 수 없게 됩니다.이런 이유로 기존 블록체인 기반 파일 저장 기술은 대용량 파일번호와는 대조적으로 큰 파일을 업로드하고자 하는 개별적이고 자유 분방한 대중 소비자에 주로 초점을 맞추고 있습니다. 블록체인 전용 저장은 기업 고객의 보안, 성능, 대기 시간 및 사용 편의성 요구 사항을 충족시키지 못합니다. Cryptyk Inc에서 개발한 CRYPTYK 하이브리드 블록체인 기술은 블록체인 전용 플랫폼에 비해 더 다양한 유형의 해커들의 공격 포인트를 줄이면서 고도로 유용한 접속 대기시간을 200ms 미만으로 나타냅니다.

뿐만 아니라,CRYPTYK 생태계는 기업 환경에 안전하고 사용이 간편하며 대기 시간이 짧은 파일 저장 플랫폼을 훨씬 더 많이 제공합니다. 또한 사용자 접속 제어, 파일 추적/로깅/감사, e-메일/채팅 보안, 내부 위협 모니터링, 정책 시행, 업계/법률 준수를 관리합니다. 이 생태계는 비지니스, 단체 또는 기업이 클라우드로 이동 하는 것에 대한 다섯 가지 주요 사이버 보안 위협(또는 공격 경로)으로부터 보호하는 단순하고 완벽한 기업 보안 및 저장 솔루션입니다. 기업 고객을 위한 단일 제품 번들에 있는 완벽한 기업 보안 및 저장 솔루션인 CRYPTYC 생태계는 다양한 기존 사이버 보안 및 저장 기술을 대체할 수 있습니다. 가장 중요한 것은 CRYPTYC 기업 고객 개개인이 기업의 문서 공유를 통해 궁극적으로 CRYPTYC 기업 고객이 될 수 있다는 점을 의미하는 CRYPTYK 생태계의 고유한 암호화 경제성입니다.

결과적으로, 이는 그들의 개별 고객이나 일반 소비자들에 의한 후속 채택을 통해 비지니스와 기업 공동체 전체에 걸쳐 더 많은 채택을 확산 시킵니다. 이것은 대중적인 고객 참여와 고객 전환을 위해 참여자 인센티브를 제공해 주는 암호화 경제의 네트워크 운영을 위한 좋은 예입니다.

CRYPTYK 에코시스템은 완벽한 보안 솔루션, 간편한 구축, 관리의 용이성 및 전반적인 비용 절감 효과를 제공합니다. 이 플랫폼은 근본적인 데이터 저장 수준 자체의 보안 문제를 해결하기 때문에 기존의 보안 및 저장 솔루션에 대한 복잡하고 단편적인 사후 접근 방식이 필요하지 않습니다. 보안 암호화는 파일 스토리지의 간접적인 보호를 위해 분산된 저장 프로세스에 기록됩니다. 또한 기업에서 제공받은 제한된 무료 저장 및 보안 서비스를 사용하는 기업의 고객(즉:개별 일반 소비자)에게도 고유한 이점이 있습니다. 생태계는 사용자 ID, 파일 업로드, 파일 공유, 데이터 무결성 및 보안 사용자 액세스 세션 확인을 위한 보상를 줘서 CRYPTYK 토큰 참가자 (또는 CTK 채굴자)에 대한 정보 처리를 더욱 촉진시킵니다. 또한 향후 플랫폼 기능의 오픈 소스 개발을 장려하고 모든 고객의 신속한 시험과 채택을 장려합니다. 아키텍처 측면에서 하이브리드 플랫폼은 완벽한 보안 및 저장 솔루션을 구성하기 위해 보안 엔진 및 사용자 인터페이스와 통합된 세 가지 서로 다른 무료 분산형 플랫폼으로 구성됩니다.

그림 1: CRYPTYK 하이브리드 보안 및 저장 플랫폼 개요



특히, 그림 1에 자세히 설명된 바와 같이, CRYPTYK 플랫폼은 (A) 암호화된 파일 저장 및 파일 공유를 위해 VAULT라고 하는 분산형 다중 공급업체 클라우드 스토리지 플랫폼 (B) 모든 사용자 액세스 세션 및 파일 트랜잭션의 불변하는 저장를 위한 PASSPORT라고 하는 분산형 블록체인 플랫폼, (C)파일 암호화 키, 트랜잭션 데이터 및 감사 로그를 저장하기 위한 분산형 데이터베이스 맵, (D)파일 저장/공유, 보안 정책, 사용자 접속 및 파일 권한을 관리하기 위한 COMMAND라는 사용자 제어 인터페이스 그리고(E)모든 플랫폼 구성 요소의 통합과 보안 정책, 사용자 접속 제어, 파일 설정, 참가자 인센티브 및 Cryptyk Token 생태계의 시행을위한 SENTRY라는 중앙 보안 엔진 및 백엔드로 구성되어 있습니다.

세개의 분산형 저장 플랫폼(다중 클라우드, 블록체인 및 데이터베이스)모두 SENTRY 보안 엔진을 통해 상호 작용하여 CRYPTYK 생태계의 모든 참여자들을 위한 상호 보완적인 작업을 수행합니다. 또한 여러 유형의 보안 위협에 대해 다양한 방식으로 보호하여 기업 고객에게 다섯가지 보안 위협에 대한 완벽한 데이터 보안 및 저장 솔루션을 제공합니다. 요약하자면, CRYPTYK 플랫폼과 CTK 생태계는 기업과 소비자 사이의 바이러스성 네트워크 효과를 활용해 모든 참여자에게 플랫폼의 채택, 성능, 보안 및 가치를 향상시키는 완벽한 기업 보안 및 저장 솔루션입니다.

2. 기술적 배경 및 과제

분산형 플랫폼은 보안과 확장 가능한 처리량 측면에서 기업 고객과 사용자에게 상당한 잠재적 이익을 제공하지만, 분산형 플랫폼의 정확한 설계와 크기는 사용자를 위한 수많은 다른 제품 성능과 가용성 특성에 큰 영향을 미칠 수 있습니다. 특히 관련성이 있는 것은 저장 노드의 유형과 개수(또는 정보 처리 노드)가 플랫폼의 잠재적 공격 포인트와 접속 대기 시간에 어떻게 영향을 미칠 수 있는가 하는 점입니다. 또한 기밀 데이터를 중앙 집중식 아키텍처에서 분산형 아키텍처로 이동하면 일반적으로 비용 효율성 측면에서 기업 고객에게 도움이 됩니다. 플랫폼 보안의 개선 가능성에도 불구하고, 분산형 보안 및 스토리지 플랫폼의 광범위한 채택은 비용을 지불해야하는 기업 고객에게 상당한 비용 절감이 있지 않는 한 매우 어렵습니다. 결과적으로, 노드 수, 공격 포인트, 대기 시간 및 비용 편익 측면에서 스위트 스폿을 확인하는 것은 분산형 네트워크 솔루션의 최적 설계에 매우 중요합니다.

2(a). 분산 시스템의 공격 포인트

분산형 저장 플랫폼에 분산되어 있는 작은 부분으로 분할된 파일 또는 데이터 페이로드는 중앙 집중식 단일 공급업체 저장 플랫폼에 저장된 데이터보다 기본적으로 더 안전합니다. 원칙적으로 스토리지 노드 수가 더 많아질수록(이런 이유로 분산도는 높아짐)

스토리지 플랫폼의 잠재적 공격 포인트는 더 작아집니다. 공격포인트는 일반적으로 가능한 모든 공격 경로(또는 사이버 보안 위협)의 합으로 정의됩니다. 먼저 노드가 n인 저장 플랫폼의 상대적 공격 포인트(ASn)을 가능한 최대 공격포인트(즉, 1과 같음)의 표준화된 부분으로 정의 하겠습니다. 또한 단일 저장 노드(즉, n=1)에 대한 다섯 가지의 개별 공격 경로의 상대적 공격 포인트가 모두 동일하다고 가정합니다.

$$AS1\ (최대) = AS1\ (a + b + c + d + e) = 1$$

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

이제 외부 위협을 제외한 모든 잠재적 공격 경로에 대해 완벽하게 보호되는 단일 소스 저장 공급업체의 간단한 예를 들어 보겠습니다. 이 경우

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

$$AS_1\ (전체) = AS_1(a) = 0.2 = 1/5$$

파일을 대신 두개의 작은 부분으로 나누어 두개의 동일한 저장 노드(예:n=2)에 걸쳐 저장하는 경우 보안 위반이 성공하려면 두 저장 노드가 모두 손상되어야 합니다. 이 경우 저장 플랫폼의 상대적 공격 포인트는 다음과 같이 개별 노드의 공격 포인트의 산물과 같습니다.

for n = 2 $AS2\ (전체) = AS1\ (a) \times AS1\ (a) = 0.04 = 1 / 25 = 1 / 5\text{^}2$

and for n = 3, $AS_3\ (전체) = AS_1\ (a) \text{ x } AS_1\ (a) \text{ x } AS_1\ (a) = 0.008 = 1 / 125 = 1 /$

일반적으로, 각 스토리지 노드의 상대적 공격 포인트가 AS1과 같다면, 전체적으로 n노드 스토리지 플랫폼의 상대적 공격 경로는 다음과 같을 것입니다.

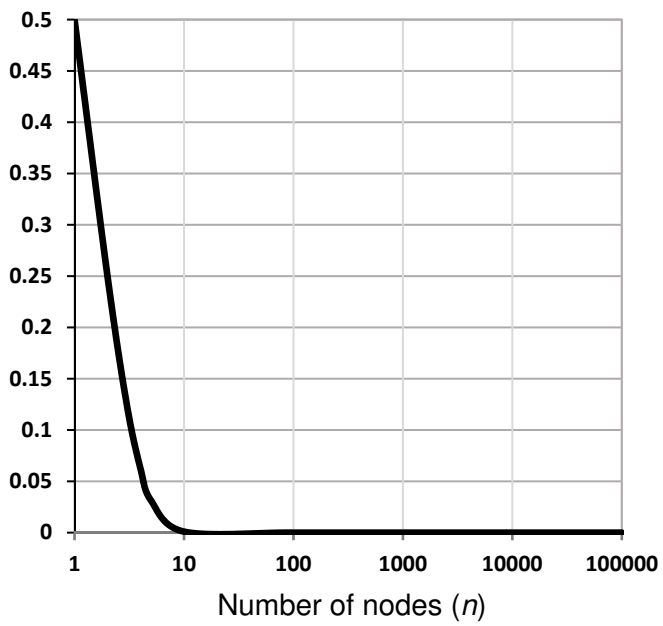
$$AS_n = (\ AS_1\ )^{\ n}$$

이제 우리가 단일 노드에 대한 상대 공격 포인트의 합계가 50%(즉, AS1=0.5)인 가장 단순한 예를 들어 보면, n노드 플랫폼에 대한 상대적 공격포인트는 다음과 같습니다.

$$AS_n = (\ 0.5\ )^{\ n}$$

그림 2a(오른쪽)는 다음과 같은 상대적 공격 포인트의 매우 점근적인 행동을 보여줍니다.

그림 2a : 공격 포인트와 노드 번호



AS1=50%인 예에서 노드수가 증가할때. 저장 노드를 다섯 개만 사용하여 상대적 공격 포인트를 4%미만으로 크게 줄일 수 있습니다. 상대적 공격 포인트는 10개 노드에 대해 약 0.1%, 100개 노드에 대해 0.0001%이하로 더 떨어집니다. 100개의 스토리지 노드를 넘어서면 공격포인트가 0에 근접하면서 무한대로 작아집니다.

결과적으로, 분산형 플랫폼 공격 포인트의 잠재적인 저감의 대부분은 상대적으로 적은 수의 분산된 독립적인 저장 노드(예:n=5–10)를 사용하여 제한된 용량으로 달성할 수 있습니다. CRYPTYC 클라우드 스토리지 플랫폼(즉:VAULT)의 설계에 있어 매우 중요한 요소는 5-10개의 저장 노드만으로도 가능한 보안 수준의 큰 향상입니다.

2(b). 분산 시스템의 대기 시간

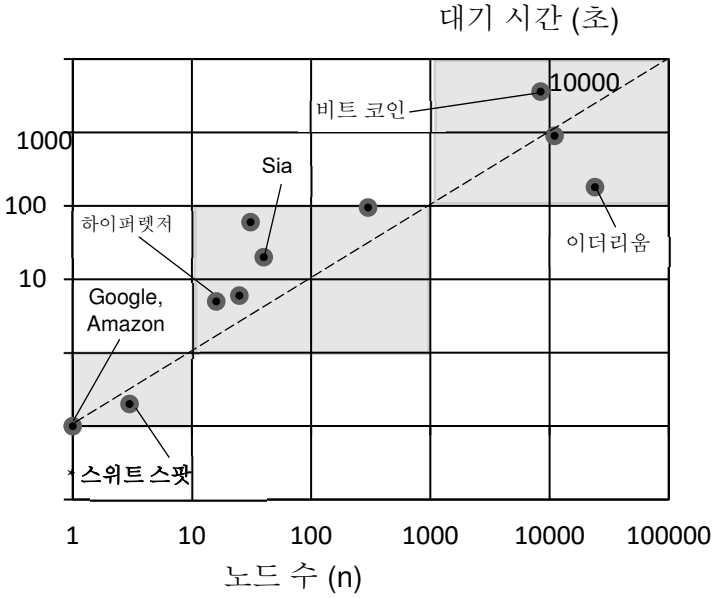
GoogleDrive, AmazonS3 및 iCloud 및 콘텐츠 전송 네트워크 같은 기존의 중앙 집중식 스토리지 플랫폼은 데이터 업로드 및 다운로드에 적정한 처리 속도를 유지하면서 접속 대기 시간이 매우 낮습니다. 접속 대기 시간은 많은 수의 작은 파일 (일반적으로 <1MB)을 자주 업로드, 다운로드 및 관리해야하는 실시간 응용 프로그램에서 중요한 성능 및 유용성 이슈입니다. 파일/폴더 관리, 파일 공유 및 실시간 편집과 같은 온라인 클라우드 기반 응용 프로그램에서는 일반적으로 실시간으로 사용할 수 있도록 수백마이크로 초 이하의 접속 대기 시간이 요구됩니다. 스토리지 플랫폼의 업로드 또는 다운로드 속도(즉:처리량)와 상관 없이, 수 초의 접속 대기시간으로 인해 대부분의 사용자가 실시간 파일 스토리지, 관리 및 편집 응용 프로그램을 사용하지 못할 수 있습니다. 클라우드 기반 스토리지 플랫폼의 대부분의 소비자와 사용자는 기존 클라우드 스토리지 서비스를 통해 업로드하는 데 1초도 걸리지 않을 작은 파일을 업로드 하는데 수십초 이상 기다리지 않으려 합니다. 결과적으로, 높은 처리량과 빠른 대기 시간을 가진 기존의 중앙 집중식 스토리지 시스템은 실시간 온라인 파일 저장, 관리 및 편집 응용 프로그램에 더 적합합니다. 이들은 공격 경로가 크고 데이터 보안 특성이 열악하다는 점에서 한가지 큰 문제만 안고 있습니다.

반대로, Si3및 Filecoin4와 같은 분산형 블록체인 저장 플랫폼은 대용량 파일 및 데이터 페이로드(즉:>100MB)의 업로드 또는 다운로드에 이상적입니다. 분산형 플랫폼은 데이터 병목 현상이나 데이터 전송 작업에 방해가 되는 운영상의 장애 가능성이 낮아 대부분의 중앙 집중식 저장 플랫폼에 비해 향상된 데이터 보안, 처리량 및 다운로드 신뢰성을 보이도록 구성할 수 있습니다. 이는 백업 저장 드라이브와 같은 다중 파일 일괄 처리 응용 프로그램을 업로드하거나 다운로드할 때 중요합니다. 이 경우 사용자는 일반적으로 완료하는데 수십 분 또는 그 이상이 걸릴 수 있는 업로드 또는 다운로드 프로세스를 시작하는데 수십 초를 기다리지 않아도 됩니다 또한 분산형 저장 아키텍처는 저장된 데이터에 높은 수준의 파일 보안을 부여하도록 설계될 수 있습니다.

그러나, 분산형 블록체인 기반 플랫폼(일반적으로 10~20초 이상)의 느린 접속 대기 시간 특성은 대부분의 개별 온라인 파일 관리, 공유 및 편집 응용 프로그램에 매우 적합하지 않다. 또한 대부분의 기업에서는 수백 또는 수천명의 직원, 클라이언트 및 고객 간에 모든 파일 저장, 편집 및 공유 응용 프로그램에 대한 완벽하고 빠른 관리가 필요합니다. 따라서 기업 환경에서 블록체인 기반 저장 플랫폼을 사용하는 것은 사용자에게는 비실용적이고 번거롭습니다.

그림 2b(오른쪽)는 노드 번호를 대비해 다양한 상용 저장 플랫폼을 측정한 접속 대기 시간을 보여 줍니다. 블록체인 플랫폼은 합의 기반 엔진의 반복 확인을 통해 모든 작업을 검증하고, 다수의 참여 저장 노드(즉:20~10,000노드)를 포함합니다. 또한 사용자가 블록체인 플랫폼을 매우 많이사용함에 따라 접속 대기 시간도 크게 늘 어날 수 있습니다. 처리량은 일반적으로 분산형 시스템의 접속 대기 시간 보다훨씬 더 나은 크기로 조정됩니다. 블록체인 플랫폼에서 합의 엔진을 구동하는데

그림 2b : 대기 시간 대 노드 번호



더 많은 노드를 사용할수록, 플랫폼에서 표시되는 접속 대기 시간은 길어집니다. 거래 중심의 비트코인 및 이더리움과 같이 널리 사용되는 블록체인 플랫폼은 현재 몇분에서 몇시간(즉:200–5,000초)에 이르는 접속 대기 시간을 보입니다. 이는 이러한 플랫폼에 사용되는 다수의 합의 노드(즉:8,000~20,000노드)에 따른 직접적인 결과입니다. 그럼에도 불구하고 이러한 매우 긴 대기 시간은 파일 저장 및 공유와 같은 대부분의 온라인 응용 프로그램에 적합하지 않지만 중앙 집중식 은행 간의 전신 송금과 같은 경쟁 금융 기술의 거래 시간에 비해 여전히 상대적으로 짧습니다. Sia 및 Filecoin(즉:20–50노드)과 같이 더 작은 노드 번호를 사용하는 블록체인은 대기 시간이 비교적 더 짧습니다(즉:10–100초). 하지만 이러한 블록체인 플랫폼의 반복적인 합의에 따른 특성으로 인해 대기 시간이 추가됩니다. 이러한 플랫폼은 백업 네트워크 스토리지 및 변경 불가능한 데이터베이스 원장과 같은 대용량 파일 저장 응용 프로그램에 매우 적합합니다. 이러한 플랫폼은 대기 시간이 어느 정도 단축되었음에도 불구하고 파일 관리, 공유 및 편집과 같은 기업에서 사용하는 실시간 온라인 응용 프로그램에서는 여전히 너무 느립니다.

그림 2b에는 GoogleDrive 및 AmazonS3와 같은 일반적인 중앙 집중식 플랫폼의 일반적인 대기 시간이 나와 있습니다(즉:단일 노드). 약 100ms 정도의 접속 대기 시간을

가지는 이러한 전용 단일 공급업체 클라우드 플랫폼은 사용자 친화적인 파일 관리 및 편집 응용 프로그램에 이상적입니다. 하지만 이러한 중앙 집중식 저장 플랫폼은 큰 공격 경로와 취약한 보안 프로파일을 특징으로 합니다. 이상적으로, 대부분의 엔터프라이즈급 파일 저장 응용 프로그램에는 처리량이 높고, 낮은 공격 포인트 및 빠른 접속 대기 시간을 제공하는 분산형 플랫폼이 필요합니다. 그림 2a (공격 포인트 대 노드 번호)와 그림 2b (대기 시간 대 노드 번호)를 비교하면 공격 포인트가 최소이고 지연 시간이 짧을 때의 절충한 스위트 스폿이 약 5 개의 스토리지 노드에 대한 노드 번호임을 알 수 있습니다 (* 스위트 스폿 그림 2b). 상대적으로 낮은 분산화의 경우, 공격 포인트는 여전히 90%이상 감소하는 반면 대기 시간도 매우 빠릅니다(즉:200-300밀리초). 따라서 5 노드 저장 플랫폼은 엔터프라이즈급 응용 프로그램의 성능과 보안간에 이상적인 절충안으로 보입니다. 하지만, 합의 기반 블록체인 플랫폼은 효과적으로 작동하기 위해 일반적으로 최소 20개의 노드를 필요로 하기 때문에 이런 비교적 낮은 수준의 분산 환경에서는 적절하지 않습니다. 5노드 온라인 저장 플랫폼의 가장 실용적인 아키텍처는 Google과 Amazon과 같은 여러 타사 클라우드 공급업체에 대한 전용 커넥션을 사용합니다.

2 (c). 기업 보안 및 저장 응용 프로그램에 대한 비용 구조

우리는 2 장 (b)에서 Sia 및 Filecoin과 같은 블록 체인 기반 스토리지 플랫폼이 접속 시간이 길기 때문에 실시간 파일 관리 및 편집 응용 프로그램에 적합하지 않은 것으로 이미 논의했습니다. 따라서 이러한 블록체인 저장 플랫폼은 데이터 백업 및 복원과 같은 대용량 파일 크기와 일괄 저장 응용 프로그램에 더 적합합니다. 그러나 이러한 대용량 파일 응용 프로그램도 이런 블록체인 저장 플랫폼은 주로 비용 구조 문제 때문에 소비자 시장에만 적합합니다. 블록 체인 기술은 많은 시장에 혼란을 줄 수 있지만 일반적으로 고객에게 큰 비용 절감이 필요합니다. 하지만 기존 클라우드 스토리지 공급업체의 온라인 저장 가격은 이미 매우 낮은 편입니다(예:TB당 사용자당 월 약 5달러). Sia와 같은 블록체인 플랫폼은 일반적으로 기존 클라우드 스토리지 공급 업체의 40-80%에 해당하는 더 저렴한 스토리지 가격을 제공합니다(예:TB당 2-4달러/사용자/월). 온라인 파일 저장을 더욱 안전하고 저렴한 블록체인 기반 플랫폼으로 이동하면 개별 소비자에게 어필할 수 있지만, 이 옵션은 기업 고객에게는 별로 매력이 없습니다.

파일 저장을 위한 완벽한 보안 솔루션을 구축하는 비용에 비해 저장 비용이 상대적으로 적게 들기 때문에 온라인 저장 비용을 절감하는 것은 기업의 결정적인 요소는 아닙니다. 분산형 플랫폼은 보안 침해에 대한 더 큰 보호를 제공하지만, 이는 외부 위협과 운영 장애에 대한 보호만을 위한 것이라는 점에 주목해야 합니다. 분산화 자체로는 내부의 바이러스 및 보안 위협에 대한 보안이 강화되지 않습니다. 모든 대기업과 조직에 있어 가장 중요한 것은 일반적으로 개별 소비자에게는 문제가 되지 않는 내부 소스(즉:직원)에 항상 존재하는 보안 위협입니다. 내부의 바이러스 및 보안 위협을 최소화하기 위해

기업은 일반적으로 사용자당 월 40-80달러의 추가 비용을 지출합니다. 전체 보안 솔루션의 주요 비용과 늘어난 대기 시간을 고려할 때 블록체인 저장 플랫폼으로 이동하는 기업이 얻을 수 있는 혜택은겨우 월 $1-$3에 불과합니다. 따라서 블록체인 기술은 비용 구조와 대기 시간 문제로 인해 기업용 스토리지 시장을 혼란에 빠뜨릴 가능성은 거의 없습니다. 그럼에도 불구하고, 기업용 스토리지를 배치할 때 보안 제품이 주요 비용 요소이기 때문에 블록체인 기술은 기업 보안 시장을 교란시킬 가능성이 매우 높습니다. 접속 대기 시간이 빠르고, 광범위한 보안 보호 기능을 제공하며, 운영 비용을 절감하는 기업 고객을 위한 분산형 저장 솔루션에 대한 수요가 상당합니다.

3. CRYPTYK 플랫폼 아키텍처

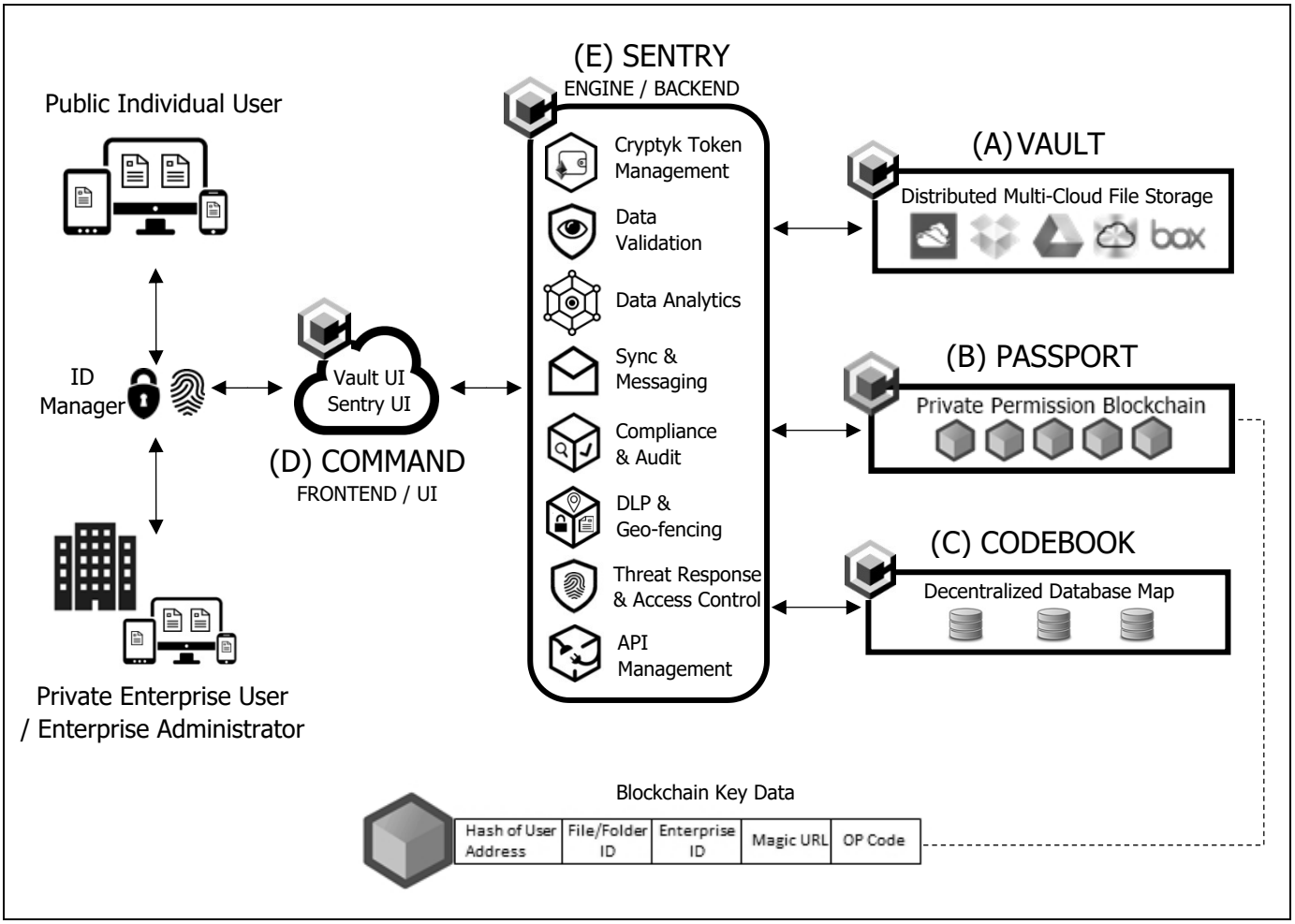
미사용 데이터 응용 프로그램에 대한 저비용 클라우드 스토리지 서비스는 복잡하고 구축 비용이 많이 소요되는 모든 기존 보안 솔루션의 근본적인 약점입니다. 완벽한 기업용 보안 솔루션을 구축하려면 클라우드 스토리지소를 최적의 보안 프로파일을 보장하는 기본 구성 요소로 통합해야 합니다. 기업 보안 및 저장 응용 프로그램에 대한 다양한 중요 성능 요구 사항을 충족하기 위해, 하이브리드 CRYPTYK 아키텍처를 뒷받침하는 설계 철학은 세가지 다른 분산형 플랫폼의 특정한 특성을 최적화하는데 기반을 둡니다. 모든 분산형 플랫폼이 모든 온라인 응용 프로그램에 이상적인 것은 아니며, 완전한 기업용 보안 및 저장 솔루션에 대한 광범위한 성능 및 가용성 요구 사항를 충족시키기 위해 세가지의 서로 다르지만 보완적인 플랫폼을 통합해야 합니다. Cryptyk 디지털 토큰 또는 CTK는 다음과 같이 CRYPTYK 플랫폼 아키텍처 전반에 핵심적인 요소입니다.

· 3개의 분산 저장 플랫폼(VAULT, PASSPORT및 CODEBOOK)을 서로 작동하고 여러 계층의 보안을 제공할 수 있도록 합니다.
· 기업 고객과 개별 사용자가 모든 범위의 보안 및 저장 서비스를 구입할 수 있도록 합니다.
· 기업 고객이 처음에 보안 및 저장 서비스를 시험 및 구축할 수 있도록 인센티브 제공한다.
· 확장 가능한 호환 API 및 플러그 인 제품을 개발하여 CTK 생태계를 지원하기 위한 오픈 소스 개발자 및 제휴 파트너에게 인센티브을 제공한다
· 생태계 참여자 및 암호화폐 채굴자가 프라이빗 블록체인 플랫폼 PASSPORT에 권한을 부여하는 CTK 보안 증명 계산을 우선적으로 처리하게 하는 인센티브를 제공합니다.

CRYPTYK 솔루션은 이미 매우 낮은 상품 수준의 가격으로 신뢰할 수 있는 저장 서비스를 제공하는 대규모 입주 기업을 대체함으로써 기존 클라우드 스토리지 시장을 교란시키려고 하지 않습니다.대신 개인 및 기업의 사용자 접속 및 파일 공유를 확인, 기록 및 관리하는 두 개의 분산된 블록 체인 보안 플랫폼을 사용하여 보다 안전한 분산형 다중 클라우드 스토리지 플랫폼 (주요 클라우드 제공업체의 기존 스토리지 서비스를 활용)을 결합합니다. 결과적으로, CRYPTYK 솔루션은 기업 보안 및 클라우드 스토리지 서비스를 포함하여 훨씬 더 안전하고 비용 효율적인 제품 번들을 제공함으로써 훨씬 더 큰 기업 보안 시장을 혼란에 빠뜨립니다. 그럼에도 불구하고 CRYPTYK 솔루션은 클라우드 스토리지만을 위한 비용 경쟁력있는 솔루션을 제공합니다.

CRYPTYK 플랫폼 아키텍처에 구축된 제품과 서비스는 CASB, CSG, DLP, 방화벽 및 위협 모니터링 제품과 같은 기업 보안 시장에서 기존 공급 업체의 다양한 고가의 제품과 서비스를 대체할 수 있습니다. 기업과 개인 고객 모두에게 이익이 되는 것은(i)보안 프로파일의 획기적 개선, (ii)단일 제품 솔루션을 통한 제품의 간단한 시험 및 배포,(iii)온라인 보안 및 저장의 총 운영 비용 절감 등이 있습니다.

그림 3 : CRYPTYK 아키텍처의 개요



CRYPTYK 플랫폼 아키텍처에 대한 개요가 그림 3에 나와 있습니다. CRYPTYK 플랫폼은 여섯 가지 주요 구성 요소로 구성됩니다. 즉,

(A) VAULT:분산되고, 사용자 암호화된, 다중 클라우드 파일 저장 및 공유 플랫폼.
(B) PASSPORT:사용자 접속/파일 공유 원장에 대한 사설 권한 블록체인 플랫폼.
(C) CODEBOOK : 내부 데이터 및 파일 암호화 키 저장을위한 분산 데이터베이스 맵.
(D) COMMAND:클라우드 기반 또는 클라이언트 기반 사용자 인터페이스 및 프런트 엔드 제어 패널/UX
(E) SENTRY : 핵심 엔진 / 백엔드가 다른 모든 구성 요소를 통합하고 모든 작업을 관리합니다.

모든 개인 및 기업 사용자는 클라우드 기반 프론트 엔드 사용자 인터페이스나 로컬 클라이언트 기반 프로그램을 통해 CRYPTYK 플랫폼에 접속하려면 Google Authenticator 또는 LastPass와 같은 다중 요소 인증 (MFA)이 있는 기존의 사용자 ID 관리 제품이 필요합니다.일반 개인 사용자에게는 제한된 보안 관리 기능과 파일 저장 공간 (즉 : 1GB의 저장 공간)을 갖춘 간접적으로 안전한 VAULT 파일 저장 플랫폼의 무료 버전이 제공됩니다. VAULT 플랫폼은 외부의 바이러스 및 운영 위협 요소에 대해서는간접적으로 보호를 하지만 내부 또는 보안 위협에 대해서는 아무런 보호기능을 제공하지 않습니다. 하지만 사용자는 감시 위협으로부터 보호하는 SENTRY 보안 엔진과 내부 위협에 맞서 강력한 보안 도구를 제공하는 PASSPORT 블록체인 네트워크를 통해 추가적인 보안 관리 기능을 구매할 수도 있습니다 (대부분의 공용 사용자에게는 문제가되지 않음). 또한 사용자는 VAULT 플랫폼에서 큰 파일 저장 용량(예:1TB스토리지)으로 업그레이드할 수도 있습니다. 개별 사용자에 대한 COMMAND 사용자 인터페이스에는 높은 개인 정보 보호를 위해 구성된 정책 설정이 있지만, 일반 사용자에게 적합한 검색은 제한되어 있습니다. 그럼에도 불구하고 파일이 개별 사용자와 공유되는 경우, 파일의 원래 작성자 또는 공유자는 사용자 그룹 내의 각 개별 파일에 대해 사용자 접속 및 파일 사용 권한을 설정할 수 있습니다. CODEBOOK 데이터베이스 맵 플랫폼은 SENTRY 엔진의 내부 데이터베이스 맵이며, 결과적으로 계정 백업 서비스를 제외하고는 사용자와 직접적인 상호 작용이 없습니다. 마찬가지로 PASSPORT 블록 체인은 일반 사용자가 알지 못하는 내부에서 작동하는 내부 불변의 원장입니다.CRYPTYK 저장 및 보안 제품 번들은 개인 고객을 대상으로하는 기존의 보안 및 저장 솔루션보다 보안성이 뛰어나고 비용이 저렴합니다.

기업 고객이 먼저 시험판을 구입한 다음 PASSPORT 사설 블록체인 보안 플랫폼과 SENTRY 보안 엔진을 포함하여 전체 저장 기능(즉:1TB의 스토리지/사용자)을 갖춘 CRYPTYK 하이브리드 플랫폼을 구입할 수 있습니다. 각 기업 고객에게는 모든 기업 직원에 대한 PASSPORT 블록체인 키 데이터에 내장된 고유한 기업 ID가 제공됩니다. 또한 기업 내의 각 사용자에게는 고유한 사용자 ID가 부여되며, 이 ID는 고유한 블록체인 키 데이터의 일부를 형성합니다. 모든 직원 또는 기업 구성원은 개별 일반 사용자와 비교하여 개인정보 설정을 줄이기 위해 기업에서 구성한 COMMAND 사용자 인터페이스 버전을 사용합니다.

이는 실제로 프라이빗 블록체인 플랫폼이 본질적으로 불투명하고, 정책 및 사용 권한에 대한 COMMAND 인터페이스 설정을 통해 사용자 지정할 수 있다는 것을 의미합니다. Cryptyk Inc는 COMMAND 인터페이스에 대한 고유한 사용 권한 아키텍처를 사용하여 역할 기반 액세스 제어 시스템을 설계, 구현 및 구축합니다. 기업 고객을위한 공인 네트워크 관리자는 PASSPORT 블록체인 데이터의 완벽한 가시성, 기업 사용자 접속 관리, 파일 접근 권한 제어, 엔터프라이즈 정책 설정, 모든 파일 공유 트랜잭션 추적 및 보안 구성의 세분화 된 선택을 허용하는 COMMAND 인터페이스의 관리 버전을 제공받습니다

Cryptyk Inc는 또한 다양한 보안 프로파일과 구성을 지정하고 적용하는 표준화된 API 형식을 설계, 구현 및 배치합니다. 미래의 오픈 소스 API 및 플러그인 개발은 서로 다른 엔터프라이즈 ID를 가진 둘 이상의 다른 기업의 내부 사용자간에 애플리케이션 인터페이스를 허용하는 산업별 브리지를 생성 할 것으로 예상됩니다. 대중적인 채택에 있어서 위해 가장 중요한 것은 기업의 직원이 기업 외부의 고객이나 개인과 파일을 공유할 때마다 고객이나 개인은 기능이 제한된 무료 버전의 VAULT 제품을 받고 일부는 궁극적으로 증가된 스토리지 및 우수한 보안 기능이 있는 유료 제품 번들로 업그레이드 됩니다. 결과적으로 기업 고객에게 완전한 CRYTYK 제품 번들을 타겟팅하면 궁극적으로 외부 고객 또는 고객과의 파일 공유 상호 작용의 네트워크 효과를 통해 저장 및 보안 제품을 채택하게됩니다. .완전한 엔터프라이즈급 저장 및 보안 제품 번들은 보안 프로파일이 뛰어나며 기업의 기존 보안 및 저장 솔루션보다 비용면에서 훨씬 저렴합니다.

4. CRYPTYK 플랫폼 구성 요소

이제 우리는 CRYPTYK 플랫폼 아키텍처를 구성하는 6가지 중요한 구성 요소의 특정 설계 파라미터, 보안 기능 및 제품 기능에 대해 논의할 것입니다.

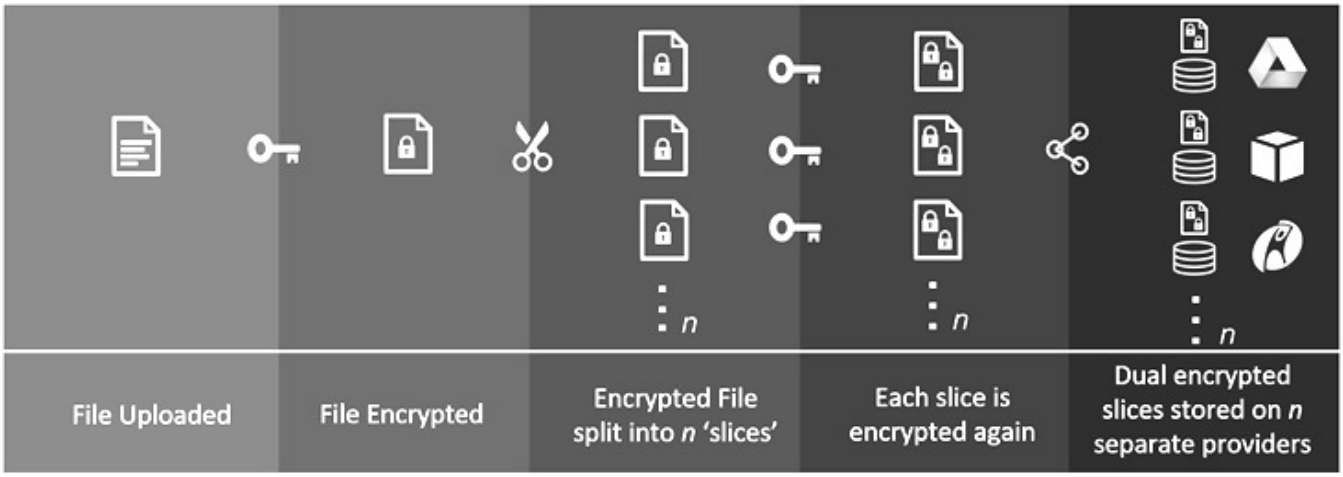
4(a). 분산 다중 클라우드 파일 저장 및 공유 플랫폼(VAULT)

암호화 형태의 생태계의 근본적인 토대는 VAULT라고 불리는 분산된 사용자 암호화 다중 클라우드 파일 저장 및 공유 플랫폼입니다. VAULT 설계는 GoogleDrive, AmazonS3, AppleiCloud, Microsoft Azure, Box, Dropbox 및 Rackspace와 같은 주요 클라우드 스토리지 공급 업체가 제공하는 다수의 전용 저장 노드(예:5 - 10노드)를 통해 제한되는 분산도를 활용합니다. VAULT의 세가지 중요 설계 특징은(1)모든 파일을 독립된 클라우드 스토리지 공급자에 별도로 저장되는 여러 암호화된 파일 부분으로 나누고,(2) 이것은 로컬 지문 인식 스마트 장치의 각 개별 파일에 대한 접속을 잠금 해제하는 암호화 키와 CODEBOOK 분산 데이터베이스 맵의 오프라인 백업부분을 저장하고

(3) 단일 클라우드 스토리지 공급자의 접속 대기 시간이 50 % - 100 % 만 느려지면서 잠재적 인 공격포인트의 90 % 이상을 감소시킵니다 (즉, 단일 공급 업체의 대기 시간 100msec에 비해 150-200msec) 따라서 개별 클라우드 스토리지 공급자의 외부 보안 침해는 여러 암호화 계층이 손상된 경우에도 저장된 파일의 작은 쓸모 없는 부분에 대한 접속만 제공할 뿐입니다. 단일 사용자의 데이터 도용은 해당 내부 사용자의 개인 장치에 대한 물리적인 접속과 CRYPTYK 사용자 계정이 모두 필요합니다. 이러한 경우에도 특정 사용자에 대해 승인된 파일만 접속할 수 있습니다. 결과적으로, 다수 사용자의 대규모 해킹은 실용적이지도 않고 실현 가능성도 없습니다.

아래의 그림 4는 분산형 다중 클라우드 파일 저장 플랫폼에 대해 선호되는 스플라이싱 및 암호화 방법을 자세히 보여 줍니다. VAULT 플랫폼으로 업로드된 각 개별 파일은 먼저 암호화된 다음 n개의 다른 파일 부분이나 조각으로 분할됩니다. 그런 다음 이러한 각 n개 조각은 다시 암호화되고 타사 클라우드 스토리지 공급 업체(예:AmazonS3, GoogleDrive또는 Rackspace)에 개별적으로 저장됩니다. 각 파일은 사용자의 개인 장치 또는 안전하고 불변하는 블록체인 네트워크에 저장될 수 있는 n+1개 암호화 키를 사용하여, n개의 독립적인 저장 공급자에 분산된 포맷으로 저장됩니다. 이 파일에 대한 접속 권한을 다른 사용자와 공유하는 경우에는 해당 사용자는 공유 파일에 대한 여섯 개의 암호화 키에 접속할 수 있는 권한이 있는 사용자 계정과 함께 VAULT의 무료 버전을 받습니다. 따라서 이 플랫폼은 매우 안전한 파일 저장 파일 공유 서비스로 효과적으로 작동합니다.

그림 4 : VAULT 파일 분할 및 암호화 방법



VAULT 플랫폼은 타사 클라우드 스토리지 공급업체를 사용함에 따른 상당한 위험을 제거하고 외부의 침해로 인한 범죄 조직의 이익을 회수합니다. 또한 바이러스 소프트웨어가 업로드되면 바이러스 또는 멀웨어 파일은 개별적으로 분할되고 암호화된 파일 부분으로만 존재함으로써 실행 프로그램을 형성하기 위한 상호 작용을 할 수 없다 . 결과적으로 이 분산형 설계는 바이러스 보안 위협에 간접적으로 영향을 받지 않으며 대기시간이 늘어나고 자주 업데이트해야하는 지속적인 바이러스 스캐닝 백신에 의존하지 않습니다

암호화 및 저장 알고리즘은 하나의 클라우드 스토리지 공급자가 작동 오류를 경험하더라도 연중무휴로 운영 신뢰성을 보장하는 중복 저장 방식(RAID 아키텍처와 유사)을 사용합니다. 이는 기존 RAID 저장 아키텍처와 유사한 방식으로 여러 저장 노드에 걸쳐 파일 부분에 엇갈린 중복성 계층을 추가하여 구현할 수 있습니다. 따라서 VAULT 플랫폼은 5가지 주요 기업 보안 위협 중 세가지(즉, 외부, 바이러스 및 운영)에 대해 간접적으로 영향을 받지 않으며, 지속적인 데이터 보호를 위해 정기적인 제품 업데이트도 필요하지 않습니다. 그럼에도 불구하고 분산형 파일 저장 플랫폼은 여전히 내부 소스로부터의 보안 침해와 개인 간의 통신에 대한 감시에 취약합니다. 내부 및 보안 위협은 모든 비즈니스, 기업 및 조직의 주요 관심사입니다. 그러나 내부 위협은 일반적으로 개별 일반 사용자에게 영향을 미치지 않으며, 보안/데이터 가로채기 위협은 여전히 이들의 가장 큰 취약점으로 남아 있습니다.

4(b) 프라이빗 블록체인 보안 플랫폼 (PASSPORT)

PASSPORT 프라이빗 블록체인 보안 플랫폼의 목적은 (a)모든 엔터프라이즈 ID, 사용자 ID, 파일/폴더ID, 사용자 액세스 세션, CRYPTYK 플랫폼의 마법 URL 및 운영 내역에 대한 영구적이고 변경할 수 없는 감사 가능한 기록을 제공하는 것입니다. (b) 퍼블릭 개인 사용자, 개인 기업 사용자 및 기업 관리자에게 파일 작성, 삭제, 편집, 검토, 업데이트 및 공유를 포함한 모든 사용자 접속 및 파일 트랜잭션 정보에 대한 사용자 지정 가능한 접속 권한(불투명도정도에 따라 다름)을 제공합니다. (c) PASSPORT 플랫폼은 처음부터 Cryptyk 플랫폼 요구 사항에 고유한 새로운 블록체인 아키텍처 및 프로토콜로 구축되어야합니다. 하지만, 그것은 또한 사설 블록체인 모드로 구성된 Ethereum이나 Hyperledge와 같은 타사 블록체인 아키텍처 위에 쉽게 구축될 수 있다. 후자의 옵션은 의심의 여지없이 배치에 가장 쉽고 비용 효과적인 솔루션입니다. 하지만 주요 타사 블록의 최신 버전은 일반 버전이며, 적절하게 안정하고 및 확장 가능한 타사 옵션은 아직 알려지지 않았습니다. 따라서 Cryptyk은 하이브리드 분산형 플랫폼의 특수한 요구 사항에 맞는 블록체인 아키텍처를 위한 가장 안전하고 사용자 지정 가능하며 확장 가능한 옵션을 개발하거나 공동 개발할 것입니다.

사용자 지정이 가능한 블록체인 아키텍처는 기업 관리자가 모든 기업 사용자 행동 및 기업이 소유한 모든 파일 전송(즉:모든 직원 파일)을 추적, 분석 및 감사할 수 있는 기능을 제공합니다. 승인된 기업 관리자의 경우, 이 세분화된 가시성은 단순히 기업 사용자를 추적하는 것을 넘어 기업 직원이 소유하거나 생성한 파일에 접속할 수 있도록 허용된 개별 일반 사용자를 추적하는데까지 확장됩니다. 또한 기업 사용자, 직원 및 개별 일반 사용자는 파일 공유 기록을 추적하고 자신이 소유하거나 생성한 개인 파일에 대한 사용자 접속을 추적하는 기능을 제공합니다. 개별 사용자는 공유하는 사용자의 특성에 따라 개별 파일에 대한 보안 접근 수준을 설정할 수 있습니다.

이러한 플랫폼 디자인을 통해 개별 파일의 생성자 또는 소유자는 광범위한 상용자 지정 보안 기능 및 사용 권한 수준으로 파일 접근 기록을 안전하게 공유, 모니터링 및 추적할 수 있습니다.

개별 일반 사용자와 개인 기업 관리자 모두에게 적합한 개인 승인받은 블록체인 보안 플랫폼 디자인은 가능한 매우 세밀한 수준으로 설정된 다양한 변수를 수용해야합니다. VAULT 파일 저장 플랫폼의 세분화된 특성과 결합된 PASSPORT 블록체인 설계의 사용자 지정 가능한 불투명 특성은 개별 파일 접속을 위한 데이터 가시성 및 데이터 개인 정보 보호에 대해 세밀하게 조정된 제어 기능을 제공합니다. PASSPORT는 개인과 기업 모두에게 다양한 국가 간의 개인 여행 활동 기록을 제공하는 국제 여권 및 비자와 유사한 방식으로 모든 파일 거래 및 사용자 활동에 대한 영구 기록을 제공합니다. 따라서 사용자 지정 가능한 검색 속성을 갖춘 블록체인 설계는 기업에 대한 내부 보안 위협을 분석, 관리 및 방지하기 위한 이상적인 보안 아키텍처를 만듭니다. VAULT 파일 스토리지 플랫폼의 수동 보안 기능과 결합된 이 블록체인/멀티 클라우드 하이브리드 솔루션은 모든 외부, 바이러스, 운영 및 내부 보안 위협으로부터 보호합니다.

블록체인 디자인 관점에서, PASSPORT 플랫폼은 보안 검증 증명이라는 새로운 형태의 합의 주도 검증을 활용합니다. 블록체인 합의 설정 및 확인된 블록체인 결과는 SENTRY코어 엔진과 백엔드에 의해 관리되고 감사되어 집니다(섹션 8e 참조). 우리는 무결성 증명(Pi), 기밀성 증명(Pa), 접근 증명(Pc), 상태 증명 (Pp) 및 준수 증명(Pc)으로 보안 증명(Ps)을 정의한다.

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

파일 또는 사용자 이벤트에 대한 보안 증명을 구성하는 다섯 가지 확인 증명은 다음과 같이 설명됩니다.

· 무결성 증명이란 파일의 무결성을 검증하는 것이며, 악성 응용 프로그램이나 바이러스 코드가 아니라는 것을 증명합니다(파일의 암호를 해독하지 않는다는 점에 유의).
· 기밀성 증명는 공격자가 파일을 복사하거나 해독하지 못하도록 하는 공격자의 시도에 대해 파일이 안전하게 보호되고 있는지를 확인하는 것입니다.
· 접근 증명은 역할 기반 접속 제어(RBAC), 위치 정보, 파일 레벨 권한 및 다중 요소 인증(MFA)의 검증 기능입니다.
· 상태 증명은 사용자 기기의 지문 스코어, 기기의 보안 상태 및 위협 보호 분석의 검증 기능이다.
· 준수 여부 확인은 준수 요건, 규정 요건, 법적 요건, 조직 정책, 절차 및 목표에 대한 검증 기능입니다.

CRYPTYK 참여자와 CTK 채굴자(또는 중개인)는 분산형 합의 주도 블록체인 엔진을 통해 특정 파일 거래 또는 사용자 작업에 대한 정확하게 증명한 것에 대해 CTK 토큰으로 보상을 받습니다.

4 (c). 분산 데이터베이스 맵 (CODEBOOK)

CODEBOOK 분산 데이터베이스 맵의 목적은(a)오프라인 백업 본사본의 모든 파일 암호화 키(VAULT에 저장된 각 파일에 대한 6개의 키)를 모든 개인 및 기업 사용자가 스마트기기나 개인 컴퓨터가 손실되거나 분실된 경우를 위해 안전하게 저장하고.(b) 모든 정책 정보, 감사 데이터, 사용자 로그, 보고서, 거래 데이터 및 준수 데이터를 안전하게 온라인으로 저장합니다. 중앙 집중식 관계형 데이터베이스와 같은 데이터베이스 맵에 대한 기존의 다양한 옵션이 존재하지만, 선호하는 솔루션은 BigchainDB10, Cockroach DB11 또는 Hashgraph12와 같은 보다 안전한 분산형 데이터베이스 원장 플랫폼을 활용해야 합니다. 보안 및 사용자 지정이 가능한 이유로 인해 이러한 데이터베이스 플랫폼은 VAULT 플랫폼과 같은 분산 파일 시스템 관리자 및 PASSPORT 플랫폼과 같은 개인 권한이있는 블록체인 원장과의 통합에 적합합니다. 모든 파일 암호화 키의 오프라인 데이터베이스 맵에 대한 기본 다운로드 구성에서는 오프 라인 서버에 대한 온라인 파일 캐시가 있는 단방향 데이터베이스 전송 메커니즘 (예 : 광 다이오드)을 사용해야 합니다. 기기가 분실되거나 손상된 고객을 위한 백업 암호화 키에 대한 접근은 특정 사용자에게 허가된 모든 암호화 키의 시간 제한 복사본의 온라인 링크로 제공되어 집니다.

4 (d). 사용자 제어 인터페이스 / 프론트 엔드 (COMMAND)

COMMAND 프론트 엔드 제어 인터페이스 목적은 (a) SENTRY 백엔드 엔진과 3 개의 분산 형 스토리지 플랫폼을 사용하여 모든 사용자에게 모든 파일 저장, 공유 및 보안 활동을 관리하기 위해 고도의 사용자 지정 가능하고 사용하기 쉬운 인터페이스를 제공하고. (b) 신용화폐 (즉: USD)와 Cryptyk 토큰 (즉, CTK) 모두로 다양한 보안 및 스토리지 제품을 지불 할 수있는 제품 구매 인터페이스를 제공합니다. 각 고객이 구입한 솔루션과 사용자 유형(퍼블릭 개인, 기업 사용자 또는 기업 관리자)에 따라 각 사용자에 대해 다양한 보안, 개인 정보 보호, 가시성 및 관리 기능이 사용되거나 사용되지 않도록 설정됩니다. 사용자 제어 인터페이스는 나머지 CRYPTYC에 접근하기 위한 클라우드 기반 또는 로컬 클라이언트 기반 사용자 인터페이스일 수 있습니다. 대부분의 일반 개인 사용자와 기업 사용자는 단순성, 장치 이동성 및 데이터 동기화의 용이성 때문에 클라우드 기반 인터페이스를 사용하도록 선택할 것으로 예상됩니다. 그러나 기업 관리자는 유기적 구조의 프로토콜과 절차로 인해 로컬 클라이언트 기반 인터페이스를 선호할 수 있습니다. 프론트 엔드에 접속하려면 Cryptyk이나 Google Authenticator 또는 LastPass 같은 타사가 개발한 MFA 응용 프로그램이 필요합니다. 본질적으로 COMMAND 프론트엔드 플랫폼은 하이브리드 CRYPTYC 플랫폼에 저장된 모든 데이터를 세밀하게 관찰하고 제어할 수 있는 보안창이나 판유리이다.

이 기능은 사용자 유형과 특정 파일, 폴더 또는 사용자 작업에 대한 엔터프라이즈 정책 설정에 따라 데이터 투명성 및 개인 정보 보호 기능을 제공합니다. 고객 관점에서 COMMAND 프론트엔드은 VAULT 파일 스토리지 플랫폼과 SENTRY 보안 엔진의 관리를 할 수 있는 두개의 보완적인 사용자 인터페이스로 나타납니다. 일체의 VAULT + SENTRY 제품 번들은 완벽한 클라우드 스토리지 및 보안 솔루션을 구성합니다.

4(e). 보안 엔진 및 백엔드(SENTRY)

Cryptyk은 SENTRY 보안 엔진과 백엔드 플랫폼을 설계, 개발 및 배포하여 (a) 기업 보안 및 저장 서비스의 대가로 토큰 채굴자에게 CTK 토큰의 공급 권한을 부여하는 데이터 관리, 로직 처리, 정책 시행, 데이터 분석 및 암호화 엔진을 제공하고,(b) COMMAND 사용자 인터페이스와 3개의 분산 스토리지 플랫폼 구성 요소 VAULT(파일 스토리지용), PASSPORT(사용자/파일 작업 로그용) 및 CODEBOOK(파일 키 백업/데이터베이스 맵용)간의 중앙 상호접속을 제공하고 (c) 합의 기반 보안증명 프로토콜 설정 관리 및 결과을 관리하고 (d) 기업 고객, 기업 사용자, 일반 개인 사용자, 고객 제휴 파트너 및 전략적 개발 파트너, 오픈 소스 개발자, 토큰 판매투자자 및 CTK 광부를 포함한 모든 CRYPTYK 플랫폼 참여자의 인센티브에 대한 CTK 생태계의 책임 있는 관리를 제공합니다.

SENTRY는 모든 암호화, 데이터 유효성 검사, 데이터 분석, 동기화, 메시징, 규정 준수, 감사, 정책 시행, 데이터 유출 방지, 지역 보안 및 위협 분석 기능을 관리합니다. 결과적으로 백엔드는 다른 모든 플랫폼 구성 요소를 둘러싸는 추가 보안 계층의 역할을 하며 이메일, 채팅 또는 트랜잭션을 보낼 때 모든 사용자를 감시 위협으로부터 보호합니다. 또한 타사 응용 프로그램 개발자, 전략적 개발 파트너, 고객 제휴 파트너 및 Cryptyk Inc에서 개발한 API와의 상호 작용을 관리합니다.가장 중요한 점은 백엔드가 고객 시험, 고객 구매, 채굴 지불, 개발자 지불, 전략적 제휴 지불 그리고 디지털 통화(이더리움과 비트코인)와 신용화폐(US 달러와 유로)의 토근 교환을 포함한 모든 CTK 토큰 생태계 활동을 관리한다는 것입니다. CTK 생태계 구조의 근본적인 목적은 CTYPTYK 플랫폼의 기업 채택을 장려하고 성장시키는 것입니다

전체 하이브리드 암호화 플랫폼(VAULT, SENTRY및 PASSPORT스토리지 구성 요소 포함)을 구매할 때 기업 고객은 먼저 플랫폼을 시험해 보고, 1TB 당 월 20 달러에서 30 달러 사이의 사용자 지정 보안 및저장 번들의 다양한 기능을 구매할 수 있습니다. 이는 여러 스토리지 및 보안 공급업체의 기존 솔루션에 비해 보안 및 스토리지 비용이 절반 이하가 될 것으로 예상됩니다. 또한 이 솔루션은 다섯 가지 주요 보안 위협에 대해 공격 포인트가 크게 감소된 기업 고객을 위한 훨씬 더 완벽한 보안 솔루션입니다.

CRYPTYK 하이브리드 번들은 Sia 및 Filecoin과 같은 블록 체인 전용 파일 저장 플랫폼과 비교하여 보안 프로필, 접속 대기 시간, 플랫폼 가용성, 제품 기능 및 비용 구조를 획기적으로 향상시킵니다.

4(f) 엔터프라이즈용 추가 스토리지 구성

VAULT 플랫폼에 대해 여기에 제시된 기본 스토리지 구성은 Amazon 및 Google과 같은 여러 타사 클라우드 스토리지 공급자의 여러 클라우드 스토리지 노드를 사용하지만 비슷한 보안 잇점을 위해 다른 유형의 저장 노드에도 고유 한 분산 사용자 암호화 스토리지 방법을 적용 할 수 있습니다 특히 중요한 것은 플랫폼이 여러개의 기존 내부 저장 서버를 저장 노드로 사용하도록 구성된 경우입니다. 동일한 기업 독립체에서 소유한 저장 서버를 사용할 경우 각 저장 노드가 서로 완전히 독립적인 다중 클라우드 VAULT 구성의 동일한 보안 수준을 제공하지 못하지만 기존 기업 서버 저장 방법에 비해 크게 향상된 보안을 제공합니다. 내부 저장 서버 네트워크에 배포된 기업 네트워크 VAULT 플랫폼은 온라인 멀티 클라우드 구성에 비해 향상된 접속 대기 시간 및 처리량을 보여야 합니다. 또한 다중 클라우드 VAULT 플랫폼을 기업 네트워크 VAULT 플랫폼과 쉽게 통합하여 데이터를 내부 기업과 클라우드 간에 손쉽게 이동할 수 있는 하이브리드 저장 플랫폼을 구축할 수 있습니다. 기업 연합에 있는 여러 기업 네트워크에 걸쳐 저장 노드를 사용하는 다른 저장 구성도 가능합니다. 그럼에도 불구하고, 원래의 다중 클라우드 VAULT 구성은 가장 안전한 옵션으로 남아 있으면서(여러 클라우드 스토리지 공급업체의 독립성 덕분에), 뛰어난 직원 이동성과 데이터 접근성을 보장합니다. 클라우드, 하이브리드, 온프라미스(기존서버 구축방식) 또는 통합 스토리지 구성과 상관 없이 VAULT 파일 스토리지 플랫폼의 기본 속성은 그대로 유지됩니다. 특히 저장 아키텍처에서 사용자가 암호화한 파일 분산 환경으로 인해 VAULT 저장 구성은 외부의 바이러스 및 운영 위협에 대한 간접적인 영향을 받지 않음을 의미합니다.

(5) CRYPTYK 토큰 관리

CRYPTYK 디지털 토큰 (예 : CTK)은 CRYPTYK 하이브리드 플랫폼을 구동하고 3 개의 분산 된 플랫폼이 서로 통신하여 고객을 위해 완벽하고 상호 운용 가능한 보안 및 스토리지 솔루션을 제공하는 데 필수적입니다. 결과적으로 CTK의 공급, 수요 및 흐름을 효율적으로 관리하는 것이 기본적인 암호화폐 경제 원칙에 따라 전체 생태계의 확장 가능하고 수익성있는 성장에 중요합니다. 디지털 토큰 생태계를 관리하기 위해 CRYPTYK Token Management (CTM) 플랫폼은 위 그림 3에 나온바와 같이 SENTRY 라는 백엔드 엔진의 구성 요소를 형성합니다.

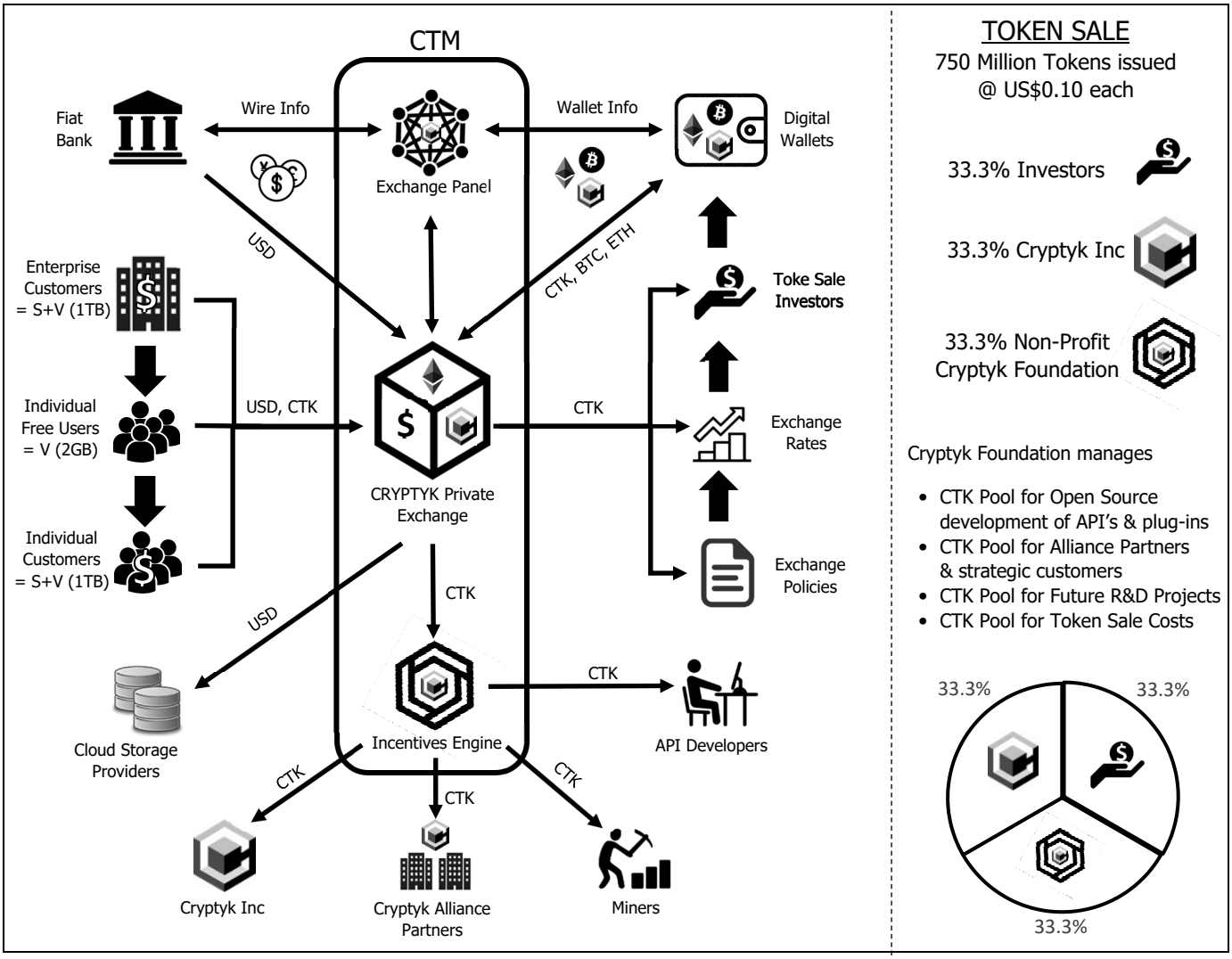
위의 그림 3에 표시된 바와 같다. CTM플랫폼의 자세한 구조는 아래 그림 5에 나와 있으며 다음과 같은 3가지 주요 구성요소로 이루어져 있습니다.

· 법정화폐은행(달러 단위) 디지털 화폐 지갑(CTK, 비트코인 또는 이더리움단위)과 연동하고 CTK토큰, 명목화폐, 디지털 통화(달러에 고정)로 이루어 지는 모든 거래를 관리하는 CRYPTK 거래소 패널.

· CRYPTYK 비공개 거래소의 기능은 아래와 같습니다. Cryptyk 제품활성화를 승인합니다. 고객 송장 및 지불을 관리하며 아마존 및 구글(달러로 고정)과 같은 클라우드 스토리지 공급자에게 비용을 지불합니다.생태계 참가자간 CTK 토큰, 법정화폐, 디지털 통화의 거래와 흐름을 가능하게 합니다.

· CRYPTYK 인센티브 엔진(Engine)의 기능은 아래와 같습니다. CRYPTYK 비공개 거래소로 부터 CTK로 수익을 받습니다. Cryptyk Inc와 CRYPTYK 채굴자간에 CTK 수익을 공유합니다. 타사 소프트웨어와 인터페이스하는 API를 구축하는 오픈 소스 개발자에게 비용을 지불합니다. 전략적 제휴 파트너에게 Cryptyk 제품을 시험 사용할 경우에 금전적 장려금을 제공합니다.

그림 5:CTM(Cryptyk Token Management) 플랫폼



성공적이고, 확장성이 있으며, 수익성이 있는 CRYPTYK 플랫폼의 경우, 토큰 판매를 위한 스마트 컨트랙 프레임워크에 따라 적절히 배부하고 발행된 CTK 토큰의 총 수를 포함하는 토큰 판매 상품의 초기 구조를 최적화해야 합니다.

토큰 판매를 하는 투자자들은 총 7억 5천만개의 CTK의 최대 3분의 1까지 구매할 수 있습니다. (예 : 초기 판매 가격으로 2억5천만 CTK, 약 10센트/1CTK).

CTK의 또 다른 2억 5천만명(33.3%)가 Cryptyk주식 회사의 주주를 위해 예약되어 있고 이들은 2년에서 4년간(설립자, 투자자, 또는 고문 등)에 걸쳐 천천히 주식을 교환할 수 있습니다. (설립자, 투자가, 고문 또는 직원 여부에 따라 다릅니다.)

나머지 2억5천만 CTK는 Cryptyk 재단이라고 불리는 비영리 단체에 의해 배포되기 위해 비축되어 있습니다. Cryptyk 재단은 CTK광부와 Cryptyk Inc 사이의 고객 매출 이익을 공유하는 Cryptyk 인센티브 엔진에 대한 규칙을 관리하고 설정을 최적화합니다.

Cryptyk 재단은 오픈 소스 API개발자, 전략적 제휴 고객, 미래 R&D 프로젝트에 대한 보상으로 보관된 2억5천만개의 CTK를 관리한다. 그리고 공개 토큰 판매에 필요한 운영경비를 지출한다. 이 3가지 토큰 생성 구조는 전략적 제휴 고객을 위한 Cryptyk 제품의 신속한 시험과 채택을 보장하고 타사 API개발자 및 전략 개발 파트너의 플랫폼 기능에 대한 오픈 소스 개발을 장려하기 위한 것입니다.

토큰의 총수는 최초 토큰발행 시 7억 5천만개로 제한되며, 결국에는 Cryptyk 재단의 책임경영과 토큰 경제성 전략에 따라 CTK의 수요가 결정됩니다. 모든 발급된 토큰의 33%를 비영리단체인 Cryptyk재단에서 소유하는 목적은 전체 CTK커뮤니티가 암호화폐 프로젝트에 참여하고 인센티브 및 보상을 규제와 관련하 업무를 투명하게 하고자 함입니다. 그것은 토큰의 적정한 희소성과 금융상의 유동성을 시장에 제공하여 CTK 시장이 점차적으로 성장하여 고객 참여를 유도하기 위한 목적도 있습니다. 궁극적으로 이렇게 하면 CTK값의 단기 가격 변동성을 줄이고 기업 고객들에 의한 플랫폼 참여함에 따라 CTK값을 장기적 상승을 유도할 수 있습니다.

Cryptyk 재단은 제휴 고객 및 전략 개발 파트너에게 토큰을 승인하고 배포하여 Cryptyk 제품의 시장 진입을 유도하고, 오픈소스 개발 커뮤니티의 성장을 육성하고 향후 플랫폼 개발 프로젝트에 자금을 조달합니다. 그것은 또한 스마트 컨트랙트 개발, 거래소 등록, 직원/팀 보너스, 통합 및 관리 비용에 대한 지급을 포함할 수 있는 모든 토큰 판매 비용과 기반 시설 설치 비용에 사용될 것 입니다. Cryptyk 재단의 2억 5천만개의 토큰은 초기 토큰 판매 4년 이내에 등록된 거래소에서 판매를 통해 완전히 소진될 것으로 예상합니다.

이 기간 동안에 모든 Cryptyk 재단에서 발급한 토큰은 잠재적인 CTK투자자, 개발자 및 고객 커뮤니티 내에서 순환되어야 합니다.

Cryptyk재단에서는 개별 API개발자 및 소프트웨어 개발자에 대해 CTK인센티브를 사용하여 Cryptyk 오픈소스 개발자 커뮤니티를 육성할 것입니다. 이 재단은 인센티브 엔진의 규칙을 검토하고 Cryptyk, Cryptyk 재단 및 CTK 채굴자 사이에 이익 공유 협약을 감독하는 책임이 있습니다. (플랫폼이 이더리움 블록체인 프로토콜을 기반으로 하는 경우에는 이더리움 채굴자가 이득을 볼 수 있습니다.) Cryptyk Inc와 CTK 채굴자는 제품 판매에서 발생한 이익의 대부분을 공유하지만, Cryptyk 재단은 생태계의 성장함에 따라 참여자들에게 분배하기 위해 충분한 규모의 CTK를 확보하기 위한 인센티브 엔진의 이익의 일부를 받습니다. Cryptyk Inc와 제휴고객 및 오픈소스 개발파트너의 중요 회원들이 참여하는 이사회가 Cryptyk재단을 관리할 것입니다. 에코시스트템은 토큰 관리를 위한 완벽한 시스템이 될 것이고, 또한 기업 고객에게 비용절감의 혜택을 제공합니다. 에코시스템은 비 고객 참여자에게 긍정적인 흐름을 제공할 것입니다. 제품의 확장성을 확보하여, CTK 가치는 장기적 성장에 도움이 될 것입니다. 장기적으로 CTK 가치의 장기적 성장은 모든 투자가, 고객, 개발자, 광부 및 제휴 파트너에게 이익이 될것 입니다.

(6) 크립토 경제성 및 토큰 가치 분석

암호화폐 플랫폼은 암호화폐-경제성 모델을 이용합니다. 이 암호화폐-경제성 모델은 분산형 네트워크 아키텍처를 목적으로 하는 두개의 서로 다르지만 무료인 사업 모델로 구성되어 있습니다. 파일 스토리지 및 공유 목적의 분산형 멀티 클라우드 플랫폼은 다음과 같은 이점이 있습니다. 1) 신뢰할 수 있는 대규모 클라우드 스토리지 업체의 빠른 액세스 지연시간 2) 최소의 공격지점 3) 대규모 확장성 4) 높은 데이터 복원력 및 저렴한 가격. 이 멀티 클라우드 파일 스토리지 플랫폼은 기업직원과 외부고객 및 클라이언트(CryptykInc. 의 무료 또는 유료 고객이 되는)사이에 파일 공유함으로써 시장성을 확보합니다. 중요한 점은 모든 파일 스토리지 비용이 미국 달러나 유로와 같은 현지 통화(법정 통화)로 지불 가능합니다.

사용자 액세스 및 파일 추적/감사 작업을 관리하기 위해 사용하는 분산된 비공개 블록체인의 주요 이점은 다음과 같습니다.

· 영구불변적으로 사용자 지정 액세스 기능 모든 사용자(기업 내, 그리고 기업과 고객)사이에서 발생하는 액세스 및 파일공유 기록에 대해 사용자 지정 가능

· 보안 위협에 대해 공격 범위 감소 모든 사용자 액세스 및 파일 공유 이벤트를 저장하는 장보 데이타베이스를 분산화 시키고, 확장가능하며, 변경 불가능하게 만들어 공경범위를 감소 시킴

· 보안 위협에 대해 공격 범위 감소 모든 사용자 액세스 및 파일 공유 이벤트를 저장하는 장보 데이타베이스를 분산화 시키고, 확장가능하며, 변경 불가능하게 만들어 공경범위를 감소 시킴

· 초기 사용자 기반 활성화 전략 제휴 파트너, 오픈 소스 개발 업체 및 CTK투자자들의 커뮤니티를 지원하여 Cryptyk 제품 및 서비스의 초기 시험과 채택을 유도

· 바이럴 네트워크 효과는 보안과 스토리지 서비스용도의 CTK 토큰 사용과 교환은 장려합니다. 하지만 암호화폐와 토큰 거래소에 등록된 바와 같이 CTK 토큰 가치 성장에 대한 투기적 투자를 장려하지는 않습니다.

· 투자자의 CTK가치에 대한 단기변동성과는 상관없이 기업 고객이 늘어남에 따라 CTK 가치는 장기적인 면에서 성장은 필연적임.

CTK 에코시스템과 모든 참여자들에게 중요한 점은 Cryptyk Inc에서 제공하는 기업보안과 스토리지 서비스 가격이 USD 또는 유로와 같은 법정통화로 고정되어 있습니다는 점입니다. 더욱이, 고객들은 CTK의 보안 및 스토리지(이걸로 통일합시다) 서비스에 대해 CTK 또는 법정화폐로 지불 할 수도 있습니다. 만약 고객이 법정화폐로 지불하기를 원한 다면, 이것은 자동적으로 Cryptyk 토큰 관리 플랫폼의 교환시스템을 통해 CTK로 변환됩니다. 결과적으로, CRYPTYK 플랫폼 사용 비용과 서비스 비용에 대한 지불을 CTK나 법정화폐로 하게 되면 토큰에 대한 수요가 증가하고, 그 결과 CTK값이 상승합니다. 더욱이, 이 설계는 고객들이 CTK토큰의 대량으로 사전에 구매하게 되면 장기적인 서비스에 대해 선불로 비용을 지불하도록 합니다.

예를 들어, 고객은 6개월 동안의 보안 및 스토리지 서비스에 대해 월100,000달러 가격으로 600,000달러로 CTK 토큰을 구매할 수 있습니다. 고객이 해당 서비스에 대해 CTK를 사전구매 하고 월별로 CTK를 지불하는 경우, CTK토큰 값은 6개월 동안 2-3배 증가할 수 있습니다. 모든 가격이 USD단위이기 때문에 CTK의 월별 가격이 1/2~1/3배 하락한 결과가 됩니다. 결과적으로, CTK 토큰을 사전구입하면 시간이 지남에 따라 보안 및 스토리지 서비스 비용이 점점 더 감소하는 효과가 있습니다.(고객수요 증가로 토큰 값이 상승한다고 가정) 제휴 파트너와 같은 초기 단계 고객들은 그들의 클라우드 스토리지 및 보안 서비스에 대해 비용을 달러로 지불할 수도 있다는 것을 알게 됩니다. 궁극적으로, 토큰의 유용성이 높을 수록 제품가격 및 CTK가격 측면에서 고객과 투자자 모두에게 더 많은 가치를 가지게 됩니다.

대부분의 암호화폐와 디지털 토큰 에코시스템의 가장 큰 문제 중 하나는 투기목적의 투자는 많고, 토큰의 유용성으로 인한 수요는 부족하다는 점입니다. 결과적으로 현재 정부 규제기관은 많은 암호화폐와 디지털 토큰을 유틸리티 토큰이나 판매용 제품 대신에 증권으로 분류하고 있습니다. 예를 들어, 주요 암호화폐인 비트코인은 가맹점에서 소매제품을 구매할 때 신용카드 및 직불카드를 대체하기 위해 개발되었습니다. 비트코인은 소매 구입비용을 5-6배 절감합니다. 은행 및 신용 카드사에 부과되는 거래당 2.5-3% 비용이 들지만, 비트코인 거래에서는 거래당 0.5-0.6% 비용이 발생합니다. 불행하게도 비트코인 생태계에서 가장 큰 문제점은 상인들이 기존의 신용카드 수수료를 지불하고 고객은 지불하지 않습니다. 상인들이 비트코인을 받으면 거래비용이 2% 절감되고 절감된 금액을 고객에게 전달할 수 도 안 할 수도 있습니다.

하지만 대부분의 소매상은 비트코인 지불을 요구하는 고객들이 많아 지게되면, 비트코인을 받을 것입니다. 소매 제품의 가격 탄력성을 고려할 때, 거래비용에서 몇 퍼센트를 절약해서는 도매상의 시장 진입을 불러올 수는 없다. 따라서 비트코인 상인 도입이 중요해 지기 전에, 비트코인으로 결제하길 원하는 대규모의 잠재고객을 먼저 확보해야 합니다. 도박이나 불법적인 상품에 대한 지불과 같은 익명성이 요구되는 분야에 비트코인 사용하지 않을 경우, 합법적인 소매품에 대해 일반 소비자가 사용하는 비트코인 양은 매우 적습니다. (합법적 소매품 분야 : 전체 비트 코인 시장 자본 총액의 몇퍼센트 정도)

결과적으로, 비트코인은 1차적인 투기적 투자 방식에 비해 소매거래 분야에서의 효용성은 매우 낮습니다. 비트코인의 주요 사용이 증권투자와 같은 것이므로, 조절 가능한 유동성 절차나 제품의 유용성이 부족하게 되면 투자 심리에 따라 비트코인 가격이 크게 변동할 수 있습니다.

반면, CRYPTYK 에코시스템은 장기적으로는 CTK 가치가 반드시 가격이 상승하게 될 것이며, 이는 증가하는 고객참여와 함께 확장될 것 입니다. 투자가들은 CTK가치로 대표되는 기업 제품에 투자하는 것이고 회사나 자산증권에 투자하는 것이 아닙니다. Cryptyk Inc는 이 기업 제품을 배송하고 CTK토큰 또는 USD를 자동으로 수락하는 가맹점일뿐 입니다. 결과적으로,CTK생태계에서는 가맹점의 채택이 필요하지 않으며, 고객 채택은 순전히 기업 시장의 대규모 수요에 의해 주도됩니다. 물론 이 시장은 더 안전하고 더 단순하며 더 저렴한 클라우드 스토리지 및 보안 제품입니다. 게다가 Cryptyk 재단이 에코시스템에 CTK를 인위적으로 공급하게 되면, 투기적인 변동성에 대항하는 시장 유동성 조정을 위한 효과적인 방법이 될 것입니다.

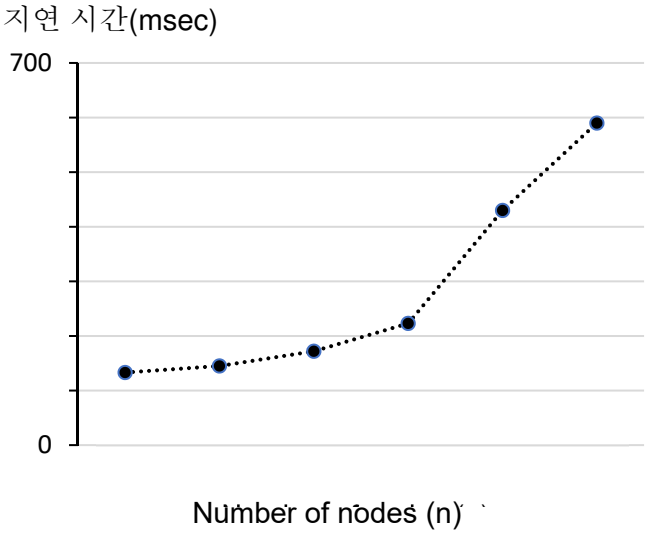
비트 코인과 달리(채굴할 때마다 자동으로 더 많은 양의 코인이 생태계에 발행됨), Cryptyk 재단은 현재 시장상황 및 생태계의 가치에 따라 고객, 개발자 및 채굴자에게 토큰발행 비율을 수동으로 증감 시킬 수 있습니다. 이러한 것은 투기적 투자자나 악의적인 참여자들에 의한 시장 변동과 CTK가치의 막대한 가격 급등에 대응하거나 최소화하는 방편이다. 비영리 Cryptyk재단은 고객참여를 장려하고, 오픈 소스 개발자 커뮤니티를 육성하며, 장기적으로 CTK 가치를 증가 시킬 것입니다.

토큰 사용의 경제적 모델링은 CTK토큰의 제품 효용이 장기적으로 총 CTK시장 자본 총액의 75% 이상 성장할 것입니다. 남아 있는 25%의 토큰은 투자자들이 투기 목적으로 사용하고 있습니다. CRYPTYK 플랫폼은 CTK커뮤니티(고객, 개발자 및 투자자 포함)들이 사용하므로써 장기적으로는 CTK가치를 안정적 성장시킬 것입니다. 타당한 평가를 통해, CTK토큰을 투자 증권이나 암호화폐가 아닌 진정한 유틸리티 토큰(또는 판매용 제품)으로 정의할 수 있습니다.

(7) 실험 결과

Cryptyk Inc가 간단한 UI를 가진 CRYPTYK 하이브리드 플랫폼과 에코시스템의 시제품 버전을 만들었습니다. 그리고 40명 이상의 초대받은 사이버 보안 전문가들이 그 시제품을 3개월 가량의 평가 기간동안 시험했습니다. 다양한 소스로 구현된 공격방법에 대해 영향을 받지 않는 것으로 입증되었기 때문에 플랫폼의 다각적 보안이람표의 무결성은 성공적으로 검증되었습니다. 외부, 바이럴, 내부 및 보안 감시 위협에 대한 공격지점의 현저한 감소를 확인했습니다다. 더욱이, 파일 업로드 액세스 지연시간

그림 6:측정된 지연 시간과 노드 개수



동작을 측정하고 일련의 노드번호(n = 3, 4, 5, 6, 7 및 8)에 대해 분석했습니다. 그림 6에서는 각 노드 구성에 대한 업로드된 5개의 통계 샘플의 평균 액세스 지연시간과 노드번호를 보여 줍니다. 3~8범위의 노드 번호에서는 130ms에서 590ms로 지연 시간이 증가하는 것으로 측정되었습니다. 이는 단일 노드 클라우드 스토리지 공급자에서 측정한 50-200ms 지연시간과 유사다. 8개 노드에 대해서도 지연시간이 용인되는 수준이지만, 이상적인 지점이 5개 또는 6개의 스토리지 노드일 경우에 더 빠른 액세스 지연시간과 공격포인트가 감소의 효과를 보였습니다.

(8) 결론

엔터프라이즈 보안 및 스토리지 용도의 하이브리드 분산형 아키텍처를 상세히 기술해 놓았다. 보안관련 성능과 액세스 지연시간의 개선을 위해 CRYPTYK 플랫폼의 단순화한 시제품 버전을 만들어서 테스트 과정을 거쳤습니다. 또한 CRYPTYK 플랫폼은 제한된 사용자 인터페이스 기능을 가지고 있습니다.기존 시스템과 비교해 볼 때 하이브리드 분산형 플랫폼에서는 보안 일람표가 크게 개선되고 공격 포인트가 크게 줄어듭니다. 이 플랫폼은 또한 3~8개의 스토리지 노드를 사용할 경우에 하위 지연시간도 상당히 개선효과가 있었습니다. 이는 시아(Sia)및 파일코인(Filecoin)과 같은 다른 블록체인 스토리지 플랫폼의 2차 대기 시간보다 훨씬 더 좋은 성능을 자랑하며, 안전한 파일 공유와 실시간 편집과 같은 실시간 기업 클라우드 애플리케이션이 가능합니다. 위의 시아(Sia)및 파일코인(Filecoin)은 장기 백업 애플리케이션에만 적합한 모델입니다. CRYPTYK 생태계는 토큰 교환과 파일 공유 활동을 통해 발생하는 바이러스성 네트워크 효과로부터 이익을 얻습니다.

결과적으로 하이브리드 아키텍처는 기업용 보안 및 스토리지 애플리케이션에 대한 보안, 성능, 지연시간 가용성 및 비용 효율성 요구를 만족합니다.

토큰 관리 에코시스템 및 토큰 경제 인프라는 또한 기업 고객, 개별 소비자, 디지털 통화 채굴자, 오픈 소스 개발자, 전략적 제휴 파트너, 토큰 판매 투자가 및 Cryptyk 주주에게 지속적으로 인센티브를 제공합니다. 많은 양의 CTK를 사용하는 참가자들에게 제공하는 인센티브가 아키텍쳐를 유지시키는 원동력입니다. Cryptyk 제품을 채택하는 고객이 많을수록 CTK토큰 부족으로 가치는 더욱 증가하게 됩니다. 클라우드 스토리지 노드 5~6개를 사용하는 완벽한 기능을 갖춘 하이브리드 플랫폼은 모든 기업에 이상적인 보안 및 스토리지 솔루션이 될 것입니다. 그것은 또한 CTK 투자자, 채굴자, 공급업체, 제휴 파트너 그리고 오픈 소스 개발자들에게 엄청난 기회가 될 것입니다. CRYPTYK 플랫폼 아키텍처와 토큰 에코시스템은 미래 비즈니스, 기업 및 대규모 조직에 중요한 보안 및 스토리지 문제를 해결하는 완벽하고 확장 가능한 저비용 솔루션이다. 다음 단계로 CRYTPYK 프로젝트에서 10센트의 최초 공개 거래가격 7억 5천만개의 토큰 중 3분의 1에 해당하는 토큰을 투자자들에게 판매할 것입니다. 단계별 토큰 판매를 성공적으로 실행후 제품 개발에 약 2,000만 달러가 소요되며, 처음에는 엔터프라이즈 도입을 통해 수십억달러 규모의 에코시스템을 만들게 된다. 이 에코시스템은 수조원 달러의 잠재적 가치로 성장할 것입니다. 현재 7천 5백만 달러 규모의 에코 시스템은 기업의 참여를 통해 수십억달러 규모의 에코 시스템으로 성장할 수 있는 잠재력을 갖고 있습니다.

(9) 참조문헌

1. 포브스 온라인 매거진(www.forbes.com)은 "2019년까지 2조 달러에 이를 것으로 예상되는 사이버 범죄 비용"이라는 제목의 기사를 게재했다스티브 모간(2016년 1월 17일)

2. 시장 및 시장 조사 분석가는 "솔루션, 서비스, 보안 유형, 개발 모드, 조직 크기, 수직이고 지역별 사이버 보안 시장"이라는 제목으로 [세계 예측2022년, (www.marketsandmarkets.com)]에 보고하고 있습니다. (2017년 7월).

3. CASB 제공자(스카이하이 네트워크, 비트를래스, 클라우드스코프)의 출판된 가격 데이터

4. "시아(Sia) : 분산형 스토리지", 데이비드 보릭 및 룩크 참파인(2014년 11월 29일)

5. "파일코인(Filecoin) : 분산 스토리지 네트워크", 프로토콜 연구소(2017년 8월 14일)

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

7. "RAID스토리지 시스템에 대한 지침서", 세임샨 퍼루말 및 피터크릿징거(2004년 5월 6일).

8. "이더리움 백서:차세대 스마트 컨트랙트와 분산화 애플리케이션 프로그램", 비탈릭 부테린 (2014년 1월)

9. 하이퍼렛져 프로젝트(Hyperledger Project), www.hyperleder.org, 오픈소스 개발프로젝트는 리눅스 재단이 관리(2015년 12월)

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).