5 월 2018

정책 방침서

버전 2.1

벼리

1. 초록

일반적이고 역사적인 경쟁, 차용된 기능 및 번역에서 잃어버린 것들과 함께 경제에 있는 통화의 의미가 연설에 있는 언어의 의미가 같다. 언어는 사용자 수와 발음 / 읽 기 / 읽음의 양 (즉, 거래)에 정비례한다. 살아있는 그대로 유지하고 그것을 멸종으로부터 구하는 것은 그것의 순환과 변화에 적응하는 다윈 주의자의 능력이다. 대부분의 전통적인 통화는 일반적으로 발전했으며 시간이 지남에 따라 공식화되고 점차적으로 채택을 통해 성공을 거두는 대부분의 방언과 유사한다. 잘 짜여진 기능과 불규칙 동사 같은 인공물의 부족으로 인해 글로벌 성공에 대한 주장에도 불구하고 구축된 언어는 실패했다.
암호화폐와 블록체인의 세계로 접어 들었으므로 변화에 적응할 수있는 능력이 플랫폼을 선호하는 거래 수단으로 만드는 것이다. 많은 알려진 블록체인은 고정적이며 어색한 디자인을 가지고 있지만 Enecuum 플랫폼은 적응력이 뛰어나고 분산되어 있으며 프로토콜 변경없이 원하는 새로운 변경 사항에 투표 할 수 있다. 필요한 경우 블록체인 매개 변수의 변경 사항을 수정된 프로토콜 버전을 통해 도입 할 수도 있다. 아래의 모든 기술적인 설명은 다음과 같은 동일한 핵심 아이디어를 공유한다. 우리는 강화된 개인 정보, 보안 및 확장성, 더 중요한 것은 Enecuum 을 유지할 미래의 블록 체인으로 변경하고 적용 할 수 있다고 믿는다.

생활하기에 만들고있다.

2. 부인

본 백서 및 관련된 문서는 Enecuum 플랫폼 ("Enecuum")의 의도된 개발 및 사용과 관련된다. 그들은 정보 목적으로만 사용할 것이며 변경될 수 있다.

- **본 백서는 예정 프로젝트에 대해 설명한다.**

이 백서에는 홍콩 법인인 주 Enecuum HK (CR: 2562183) (이하 "회사")의 신념과 회사가 제공 한 특정 가정 및 회사 정보가 포함되어 있다.

이 백서에서 살펴본 Enecuum 은 핵심 관리 및 기술 기능을 포함하여 (이에 국한되지 않음) 개발되고 지속적으로 업데이트되고 있다. ENQ 토큰 ("ENQ")은 실험 플랫폼 (소프트웨어)의 개발 및 사용과 관련이 있으며 목표를 성취하지 못하거나 달성할 수없는 기술은 본 백서에 명시되어 있다.

Enecuum 이 완료되면 본 백서의 네트워크와 크게 다를 수 있다. 미래 계획 또는 전망에 대한 성취 또는 합리성에 대한 진술이나 보증은 없으며 이 문서의 어떤 것도 미래에 대한 약속이나 진술로서 신뢰되거나 의존해서는 안된다.

- **규제 제품 제공 없다**

ENQ 는 관할 지역의 보안 제품 또는 기타 규제 제품을 대표하지 않는다.

이 문서는 유가 증권 또는 기타 규제 제품의 제공이나 권유 또는 투자 목적의 홍보, 초대 또는 권유를 구성하지 않는다. 구매 조건은 금융 서비스 제공 문서 또는 어떤 종류의 안내서가 될 수 없다.

ENQ 는 플랫폼, 소프트웨어 또는 회사 또는 플랫폼 또는 기타 공공 또는 민간 기업, 회사와 관련된 다른 회사 또는 재단 또는 기타 관할권의 기관 또는 지적 재산의 자본, 수익 또는 소득에 대한 형평, 주식, 단위, 로열티 또는 권리를 나타내지 않는다.

- 본 백서는 조언이 아니다

본 백서는 ENQ 구입할 조언이 아니다. 계약 또는 구매 결정과 관련하여 의존해서는 안된다.

-

- 위험 경고

ENQ 를 구입하고 Enecuum 에 참여하면 중대한 위험이 따른다.

ENQ 를 구입하기 전에 다른 문서에 나와있는 것을 포함하여 위험을 신중하게 평가하고 고려해야한다.

- 회사의 견해

이 백서에 제시된 견해는 Enecuum 의 견해이며 모든 관할 지역의 정부, 준 정부, 기관 또는 공공 단체 (관할 구역의 규제 기관을 포함하되 이에 국한되지는 않음)의 공식 정책이나 지위를 반영하지 않는다.

본 백서에 있는 정보는 회사가 신뢰할 만하다고 판단하는 출처를 기반으로하지만 그 정확성이나 완전성에 대한 확신은 없다.

- 본 백서의 공식 언어는 영어이다

본 백서 및 관련 자료는 영어로만 제공된다. 모든 번역은 참조 목적으로 만 사용되며 회사 또는 다른 사람이 인증하지 않은 것이다. 모든 번역의 정확성과 완전성에 대한 아무 보증도 할 수 없다. 번역본과 본 백서의 영어 버전간에 불일치가 있을 경우 영어 버전이 우선하다.

- 제 3 자의 제휴나 보증이 없다

본 백서에 있는 특정 회사 및 플랫폼에 대한 참조는 설명의 목적으로만 사용된다. 회사 및 / 또는 플랫폼 이름 및 상표의 사용은 해당 제 3 자와의 제휴나 보증을 의미하지 않는다.

- 필요한 전문적인 고문을 구해야한다

ENQ 를 구매하거나 Enecuum 네트워크에 참여할 것을 결정하기 전에 필요한 경우 변호사, 회계사, 세무 전문가 및 / 또는 기타 전문 고문과 상담해야한다.

3. 소개

2009 년에 비트코인을 창안부터 블록체인 기술은 세계 경제의 진화를 위한 새로운 전망을 열었다. 이후 스마트 계약의 출현은 사전 결정된 조건에서 신뢰할 수있는 자동 트랜잭션을 촉진하여 이 기술의 잠재적인 응용 가능성을 크게 확대시켰다. 블록체인은 무역, 금융 시장, 투표 및 물류와 같은 금융 및 경제 활동의 여러 분야에 혁명을 일으킬 수 있다고 믿는다.

오늘날 거의 모든 선도 기관들이 최고의 솔루션을 개발하기 위해 경쟁하고 있다. 가장 큰 은행과 기업은 컨소시엄을 구성하고 정부는 이 기술을 지원하기 위한 적절한 법적 틀을 만드는 방법을 모색하고 있다.

기존 솔루션과 이더리움이 가장 탁월한 솔루션 중 하나이며 이미 스마트 계약과 함께 블록체인 기술을 적용 할 수있는 충분한 기회를 제공한다. 그럼에도 불구하고 본 기술의 추가 개발 및 대중화를 위해서는 확장성, 보안 및 개인 정보 보호라는 세 가지 범주로 분류할 수있는 여러 가지 문제를 극복해야한다.

3.1. 확장성

분산형 블록 체인 시스템의 단점은 제한된 대역폭이다.
실제로 분산 원장이 사용하는 대부분의 컨센서스 구축 메커니즘은 초당 많은 트랜잭션과 네트워크 집중화 수준 사이에서 절충점을 제시한다 [1]. 따라서, 처리된 트랜잭션의 수를 증가시키고 자하는 욕구는 종종 시스템 신뢰성과 관련된 위험을 증가시킨다. 그리고 블록체인의 크기가 커지면 더 많은 디스크 공간, 강력한 인터넷 연결 및 높은 계산 능력이 필요하다. 이 모든 것이 전체 노드의 수가 감소하고 전체 네트워크의 보안에 부정적인 영향을 미칠 수 있다 (cf. 5).

3.2. 보안

확장성 관련 문제 외에도 블록체인 아키텍처 자체의 다양한 기능에 의해 생성되는 여러 가지 위협이 있다. 예를 들어, Proof-of-Work 기반으로 하는 거래 확인 메커니즘은 한 위치에서 높은 수준의 채굴 용량 집계로 이어질 수 있다. 예를 들어, 중국 본토에서 전력의 비용이 세계에서 가장 낮은 비트코인 광산 채굴 능력이 집계되었다.

이 사실은 시스템의 중앙 집중과 관련된 다양한 위험을 크게 증가시킵니다 (예 : "51 % 공격"을 수행 할 수있는 기회).

보안에 대한 또 다른 위협은 블록체인 자체보다 취약성 및 버그의 영향을 받기 쉬운 스마트 계약과 관련하여 발생하며 이미 사용자에게 수백만 달러의 손실을 초래하고 업계에 피해를 입혔다.
우리는 사용하는 스마트 계약의 수가 계속 증가 할 것으로 기대하는데 약한 반점을 확인하는 기존의 방법은 여전히 부적절하다.

요즘 또 다른 중요한 문제는 집중화가 블록체인 방향 및 제어에 미칠 수있는 영향이다. 이것은 핵심 프로토콜에 대한 수정에 영향을 미칠 수있는 소그룹의 사람들이 전력 집중화를 수행하는 곳에서 발생할 수 있다 [2]. 이 그룹의 의견이 지역 사회의 이익에 위배되는 경우에 이것은 안정적인 개발에 필요한 시스템 현대화 프로세스를 완전히 마비시킬 수있는 갈등을 초래할 수 있다. 커뮤니티와 블록 체인은 갈라질 수 있다. (cf. 5).

3.3. 개인 정보 정책

일부 블록체인 시스템은 모든 거래의 투명성을 위해 노력한다. 그러나 이 기능은 상업적 매력을 제한하고 개인 정보를 침해한다. 투명성은 분산 레지스트리의 주요 이점 중 하나이지만 특히

비즈니스 상대, 특정 금융 거래 및 사용자가 사적이고 기밀로 유지하는 것이 합법적으로 선호되는 다른 거래 간의 전송에 있어서는 이 속성이 항상 바람직한 것은 아니다.

우리는 이러한 문제가 수십개의 서로 다른 프로젝트에 종사하는 수많은 개발자들에 의해 직면하고 있다고 본다. 결과적으로 점점 더 많은 즉석 블록체인 플랫폼이 다양한 분야의 특정 작업을 해결하기 위해 매일 설계된다. 이것은 다른 유형의 분산 네트워크의 상호 운용성과 관련된 다른 문제를 야기하며해결하기 위해 이미 시작된 몇 가지 교차 사슬 프로젝트가 있다

그럼에도 불구하고 하나의 프로토콜에서 앞서 언급된 문제들을 효과적으로 해결하는 범용 솔루션이 아직 도입되지 않았다. Enecuum 은 일상 생활에서 분산 레지스트리 기술의 모든 장점을 완전히 실현할 수있는 근본적으로 새로운 구조를 기반으로 한 블록체인 시스템인 Enecuum 을 사용할 수 있다고 확신한다. (cf. 5).

4. 상품 설명

Enecuum 은 차세대 분산형 블록체인 플랫폼으로 설계되어 다수의 안전하고 확장성이 뛰어난 블록체인 서비스 및 분산 응용 프로그램을 구현할 수있는 고유 한 기능을 제공한다..

다른 플랫폼에 비해 Enecuum 의 주요 이점 중 하나는 "HyperDAG"가 블록체인 기술의 실제 응용 프로그램에 새로운 기회를 제공하는 유연한 설정으로 거래 저장 및 쓰기를위한 데이터 모델이라는 것이다. HyperDAG 는 많은 수의 거래를 저렴하고 신속하게 처리할 수있는 기능을 포함하여 수많은 잠재적인 업체 문제를 해결하기 위해 규칙을 조정할 수있는 별도의 지점을 만들 수 있도록 지원한다. 또한 이 솔루션을 사용하면 확장성 문제를 성공적으로 해결하는 '샤딩'기술을 통합 할 수 있다.

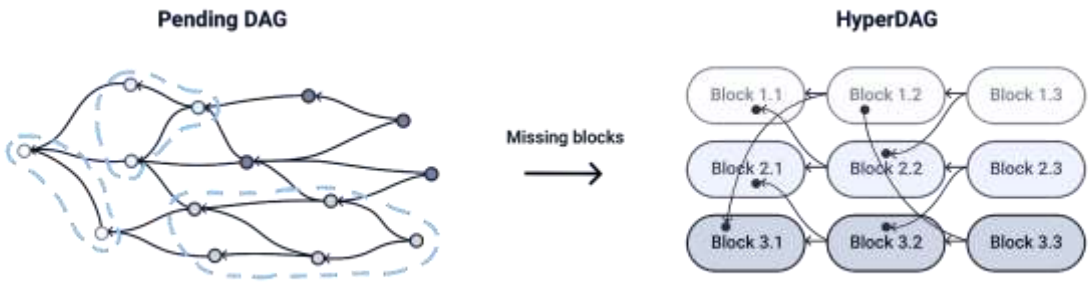

그림 1. HyperDAG 의 일부인 DAG 보류 중

Enecuum 은 일치 메커니즘의 일부로 Proof-of-Work ("**PoW**") 알고리즘 [3], Proof-of-Stake ("**PoS**") 알고리즘 [4] 및 Proof-of-Activity ("**PoA**") 알고리즘을 [5] 결합한 하이브리드 컨센서스 알고리즘을 사용한다. *PoA 는 Enecuum 을 통해 실제 상황에서 처음으로 적용되도록 제안되었다.* 합의 메커니즘의 조합을 사용하면 네트워크에 연결된 거의 모든 장치에서 거래를 확인할 수 있다. 이는 결국 시스템의 가능한 최대 분산화로 이어지고 Enecuum 은 다양한 유형의 공격에 대해 높은 내성을 갖는다.

Enecuum 은 Enecuum 플랫폼에서 작동하기 위해서 "SHARNELL 스마트 계약"[20]를 개발했다. 이러한 계약은 수식과 업체 지향 선형 논리로만 구성된다. SHARNELL 스마트 계약은 Enecuum 내의 높은 보안 수준에 기여하고자한다.

선형 로직은 시스템에 잠재적인 취약성, 오용, 정지, 교착 상태 및 기타 바람직하지 않은 결과를 크게 줄임으로써 시스템에 게시하기 전에 스마트 계약을 신뢰할 수있는 자동 인증을 허용한다.

Enecuum 의 다른 장점은 적응력이 뛰어난 시스템이라는 것이다. 사용자는 개발에 참여하고 시스템 기능 향상을 위한 다른 참가자의 제안에 투표 할 수 있다. 시스템 매개 변수의 변경을 고려하는 두 가지 방법이 있다.

- GitHub 에서 프로젝트 저장소를 브랜치하고 수정된 버전의 프로토콜 (숙련된 개발자가 사용하기 쉽다) 제시하기; 또는
- 프로토콜 수정이 필요없는 네트워크 매개 변수 조정에 투표하기.

후자는 시스템 아키텍처에 의해 제공되며 ENQ 의 모든 소지자가 사용할 수 있다. Enecuum 에서 작동하도록 제안된 기본 암호화된 디지털 토큰이다. 테스트 기간이 끝나면 사용자가 Enecuum 의 합의 모델에 대한 변경 사항을 제시 할 수 있도록 투표 알고리즘이 제안된다. 테스트 기간 동안 Enecuum 팀은 테스트 및 디버깅 목적으로 프로토콜에 대한 제어권을 유지할 것을 제안한다.

Enecuum 은 실행의 안정성과 부작용 가능성을 줄이기 위해 사용된 프로그래밍 언어 인 하스켈을 사용하여 개발되었다. 핵심 암호화 프로토콜인 Cryptonight [6] (Keccak + AES + X11)의 맞춤형 버전이 특정 용도의 집적 회로 ("**ASIC**") 장치에 대한 높은 저항성 때문에 선택되었다.

ENQ 는 Enecuum 의 기본 토큰이다. ENQ 는 시스템 특정 매개 변수에 따라 생성되도록 제안되며 계산 능력을 소비하는 보상으로 광부에게 지급된다. ENQ 는 수수료없이 송수신 될 수 있다. 스마트 계약서를 네트워크에 게시하고 스마트 계약서에서 복잡한 수학 계산을 수행하고 사용자 지정 매크로 블록, 새 토큰 및 지점을 만들고 PoS 채굴에 참여하는 데 사용할 수도 있다.

4.1 거래

우리의 견해로는 분산된 레지스트리에 거래를 저장하는 두 가지 방법이 있다.

- 블록으로(비트코인, 이더리움 및 기타); 및
- 비순환 방향 그래프 ("DAG") - (IOTA, Byteball, Universa).

전자의 장점은 네트워크의 모든 노드에서 100 % 레지스트리 중복을 통해 높은 안정성을 달성한다는 것이다. 그러나 이러한 접근 방식은 네트워크 속도 및 확장성에 특정 제한을 부과한다. 후자의 경우 DAG 에는 블록이 없으며 모든 새로운 들어오는 거래는 이전에 확인된 여러 개의 블록을 효과적으로 확인한다. 결과적으로 이 유형의 레지스트리는 많은 양의 거래를 신속하게 처리할 수 있지만 보안 수준이 커뮤니티에서 특정 관심사를 제기한다 [12].

우리는이 두 가지 접근 방식을 결합하여 "HyperDAG"라는 거래를 기록하는 근본적으로 새로운 방법을 만들었다. DAG 와의 주요 차이점은 시스템에 들어가는 거래가 단일 이전 거래뿐만 아니라 블록에 상주하는 그룹 (그림 2)을 참조할 수도 있다는 것이다. 이러한 방식으로 HyperDAG 는 두 가지 접근 방식의 장점을 성공적으로 결합하고 동시에 위에 설명된 중요한 단점을 보완하여 초당 수천 건의 거래를 처리하고 공격에 대한 높은 수준의 암호화 보호를 수행 할 수 있다.

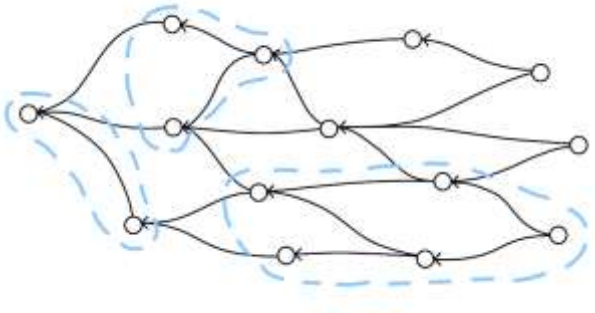

그림 2. HyperDAG 의 원리 : 인접 거래는 블록으로 그룹화됨.

거래를 나타내는 이러한 방법은 정렬, 분석 및 샘플링을 위한 방대한 기회를 제공한다. 예를 들어 한 네트워크의 프레임에 서로 다른 분기 (블록체인)를 만들고 네트워크 속도를 높이고 모든 노드에서 100 % 레지스트리 복제가 필요없는 샤딩 기술을 적용 할 수 있다.

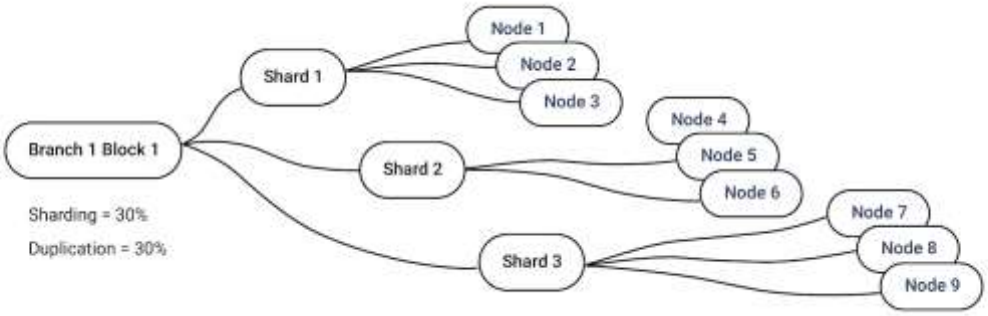

그림 3. 샤딩

Enecuum 에서 거래에는 복제, 샤딩 및 서비스 품질 ("**QS**"라고하며, 우리의 경우 거래의 속도)과 같은 몇 가지 매개 변수가 포함되도록 제안된다. 복제는 시스템의 전반적인 보안을 향상 시키지만 네트워크 속도는 감소시킨다. 샤딩은 반대 효과를 낸다. 기본적으로 복제에는 30 %, 샤딩 - 30 %, QS - 없음이 제공된다.

이러한 설정을 변경하는 옵션은 시스템의 개별 분기 내에서 고유 한 서비스를 쉽게 확장하고 만들 수 있도록 한다.

4.2 블록

HyperDAG 가 블록을 어셈블하기 시작하기에 충분한 수의 거래를 축적하는 순간 블록 생성 프로세스가 시작된다. 각 거래의 지정된 매개 변수를 분석하여 광부는 시스템에 대한 값을 판별하여 해당 블록에 추가한다. 이전 거래 [MD1]에 대한 이중 해시 링크가 도입되어 여러 거래를

포함하는 최대 n 개의 블록을 동시에 채굴 할 수 있으므로 기본적으로 거래 처리량이 n 배로 증가한다. n 의 한계는 동적이며, 예를 들어, *1000, 1000 x 62 x 40 = 2,480,000* 초당 거래 수 결과로, *40* 은 가장 작은 블록의 최대 거래 수, *62* 는 PoA 의 팀에 장치 수 (총 64 명의 팀 구성원), *1000* 은 동시에 채굴되는 블록 수이다.

Enecuum 에서 블록 크기는 고정 값을 갖도록 제안되지 않았으며 4KB 에서 4MB 까지 다양 할 수 있다. 기본적으로 최소 크기 블록을 생성하여 작업 당 최소 지연 시간에 도달 할 수 있으며 네트워크로드가 증가하면 블록 크기도 증가한다. 사용자가 4MB 보다 큰 크기의 블록을 필요로하는 상황에서 시스템은 또한 임의의 수의 블록을 매크로 블록으로 결합하는 것을 지원하므로 블록체인에 많은 양의 데이터를 저장할 수 있다.

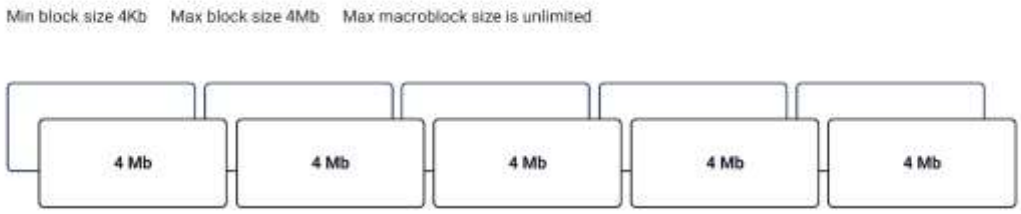

그림 4. 다양한 블록 크기

NG 비트코인 프로토콜은 블록 생성 사이의 대기 시간을 줄이기 위해 Enecuum 매크로 블록 [12]에 도입되도록 제안되어 매크로 블록 내부의 각 마이크로 블록이 실시간으로 생성되고 도착 즉시 블록 체인에 거래를 추가한다. 이렇게하면 매크로 블록이 완료되고 해시가 발견되어 네트워크상의 모든 노드간에 동기화 될 때까지 기다릴 필요가 없는데 마이크로 블록은 매크로 블록 내에서 동시에 생성 될 수 있다.

구조적으로 블록은 다음 그림과 같이 3 개의 주요 섹션으로 구성된다.

그림 5. 블록 구조

4.3 지점

거래를 저장하고 적용하기 위해 HyperDAG 를 사용하면 동질적인 거래만 포함하는 분기(블록체인)를 만들 수 있다. 각 지점은 본질적으로 별도의 블록체인이며 동시에 전체 시스템의 일부이다. 각 지점은 새로운 블록을 만들고 확인하는 고유한 규칙을 지시 할 수 있다. 노드는 모든 보조 Enecuum 지점을 복제하지 않는다.

개략적으로 지점별로 블록을 할당하는 프로세스가 그림 6 에 나와 있다.

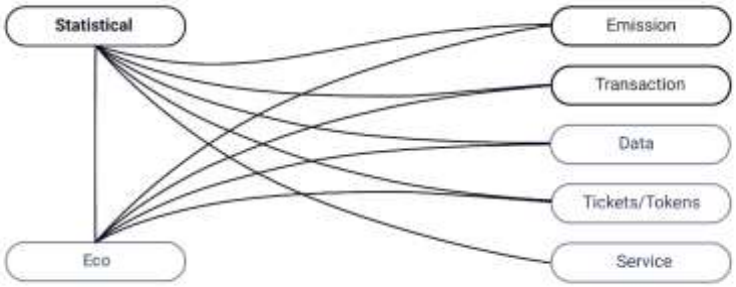

그림 6. 다른 지점에 다른 블록 할당

시스템의 주요 지점은 다음과 같이 제안된다.

1. 거래 지점은 ENQ 사용자 간의 모든 통상 거래를 포함하는 것을 목표로 한다.

2. 새로운 ENQ 를 창출하는 거래를 광업 보상으로 포함하는 것을 목표로하는 배출 지점이다.

3. 시스템의 운영에 대한 통계를 축적하고 분석하는 것을 목표로하는 통계 지점이다. 이 지점은 전체 노드 수, 마이닝 레코드, 블록 크기 및 PoA 마이닝 보상 크기를 비롯한 여러 매개 변수가 있다.

또한 Enecuum 은 아래에 설명된 다른 지점의 생성을 지원할 것을 제안한다.

1. 생태계는 의심스러운 작업과 유효성 검사에 실패한 트랜잭션을 걸러냅니다. 예를 들어, 새로 생성 된 지갑이 비정상적으로 많은 양의 트랜잭션을 보내는 경우, 먼저 상세한 분석을 위해 생태 지점으로 이동합니다.

2. 티켓 지점은 티켓을 통해 다양한 시나리오를 구현할 수있는 기회를 제공합니다. 티켓은 "티켓 지점"(참조 4.6)이라고하는 전용 사설 블록 체인 지점을 만들고 액세스 할 수 있도록하기위한 것입니다. 예를 들어, 사용자가 Ticket 을 작성하고 해당 Ticket 분기에 Token 을 발행하면이 Ticket 과 관련된 모든 조작을 암호화하여이 전용 분기에 저장할 수 있습니다. 또한 이러한 티켓 분기에는 자체 규칙이있을 수 있습니다. 예를 들어 모든 노드가 유효한 것으로 인식 될 수 있으며, 차례대로 모든 네트워크 구성원간에 합의가 필요하지 않으므로 트랜잭션이 훨씬 빠르게 처리 될 수 있습니다.

3. 서비스 지점은 폴링, 측량, 인스턴트 메시징, 문서 관리 등과 같은 분산 된 서비스를 제공하고자합니다. 서비스 지점의 트랜잭션은 추가 정보를 포함 할 수 있으므로 블록 체인을 사용하여 수많은 비즈니스 문제를 해결하기에 충분한 수준의 유연성을 확보 할 수 있습니다.

4. 분산 된 리포지토리로 작동 할 수있는 데이터 분기. 기본 원칙은 BitTorrent 프로토콜의 원칙과 비슷하지만 Enecuum 은 기존 해싱 대신 완벽한 해시 알고리즘 인 자체 솔루션을 제안합니다. BitTorrent 에서 수행 할 수없는 해쉬 테이블을 노드간에 다시 공유하거나 공유하지 않고도 암호화 된 파일의 일부 크기에 대한 권한이있는 액세스를 가능하게합니다.

4.4하이브리드 컨센서스 알고리즘(PoW, PoA, PoS)

Enecuum 에서는 Proof-of-Work ("PoW"), Proof-of-Activity ("PoA") 및 Stake-of-Stake ("PoS")와 같은 세 가지 마이닝 알고리즘 간의 상호 작용을 통해 합의가 이루어질 것을 제안합니다. . 이러한 조합을 통해 높은 수준의 네트워크 분산을 달성하면서 네트워크 보안 수준과 속도를 크게 높일 수 있습니다.

Enecuum 에서 구현하기 위해 제안 된 트랜잭션 확인 프로세스는 크게 위에서 언급 한 알고리즘에 해당하는 3 단계로 나눌 수 있습니다.

단계 1:

첫 번째 단계에는 두 가지 접근 방식이 있습니다. 보통의 경우는 PoW 네트워크에 연결된 광부가 다양한 크기의 블록에 대해 해시를 계산하며 각 블록은 자체 블록에 대해 병렬로 해시를 계산합니다. 복잡성에 대한 현재 요구 사항을 충족하는 해시가 발견 된 후 광부는 트랜잭션을 블록에 채우고이를 PoA 광부의 트랜잭션 검증과 관련된 두 번째 단계의 네트워크로 변환합니다. 두 번째 접근법은 PoW 광부가 해시를 계산하고, 매크로 블록을 생성하고 PoA 광부 팀이 트랜잭션을 포함하는 마이크로 블록으로 채우도록 열어 두는 것입니다.

Figure 7. Hybrid consensus algorithm

단계 2:

두 번째 단계에서 팀으로 나뉘어 진 PoA 광부는 선택한 PoW 시나리오에 따라 작동합니다. 위에서 설명한 첫 번째 PoW 시나리오의 경우 변환 된 블록의 헤더에서 해시를 확인하고 블록에서 트랜잭션을 확인합니다. 두 번째 PoW 시나리오의 경우 변환 된 블록의 헤더에서 해시를 확인하고 마이크로 블록을 만들고 트랜잭션으로 채우고 PoW 광부의 매크로 블록으로 보냅니다.
전체적으로 한 팀이 각각 40 개의 트랜잭션을 포함하는 62 개의 마이크로 블록을 마크로 블럭에 보냅니다. 그런 다음 블록에 포함 된 트랜잭션에 따라 PoA 광부가이를 시스템 지사 중 하나에 연결합니다. 블록 해시가 정확한지 확인하는 데는 큰 계산 기능이 필요하지 않으며이 작업은 휴대 전화를 포함한 단순한 장치로도 수행 할 수 있습니다.

마이크로 블록 생성에도 동일하게 적용되어 트랜잭션 및 트랜잭션 검증으로 채 웁니다. PoA 팀 구성 프로세스에는 팀에 들어가기위한 해시 계산이 포함됩니다. 각 팀은 최대 64 명의 참가자를 보유 할 수 있으며 노드의 지리적 위치 및 기타 매개 변수를 비롯한 여러 매개 변수를 분석하여 구성되어 가장 높은 합의 보안 수준을 달성합니다.

단계 3:

세 번째 단계에서 PoS 광부는 시스템의 모든 지갑 잔액을 지속적으로 다시 확인합니다. 이 활동을 위해, PoS 광부는 광산 보상의 일부분을 배출량의 형태로 제공하도록 제안됩니다. 보상은 두 가지 방법으로 광부의 잔액에 달려 있습니다. 첫째, 광부가 보상을받을 수없는 최소 및 최대 균형 임계 값을 정의하고 두 번째로 PoS 광부의 균형이 최소값에서 증가함에 따라 보상이 증가합니다 최대

임계 값.

네트워크가 새로운 동전을 즉각적으로 생성하는 기존의 보상 방법과 대조적으로

유효한 블록을 발견하면, Enecuum 은 현 단계에서 Wallet 잔액에 추가되는 Marks (4.6 참조)를 발행하는 반면, 실제 광산 지불은 평균 1 일 1 회 수행됩니다. 이 방법으로 시스템은 마이닝 알고리즘에 대한 가능한 공격으로부터 보호됩니다.

(예 : ASICS 를 통해) 계산 능력의 대부분을 제어하려고 시도 할 때

채무 보상은 기본적으로 PoA - 70 %, PoW - 20 %, PoS - 10 %와 같이 참가자들 사이에 분배됩니다. 그러나 통계적 지부 (4.3 참조)가 존재하면 시스템은이 분배 체계를 통제 할 수있게되어 이익을 학대로부터 보호한다.

4.5 SHARNELL 스마트 계약

Enecuum 의 Smart Contracts 는 JavaScript 로 작성되고 Google 의 V8 엔진에서 실행되도록 제안되었습니다. 시스템은 두 가지 유형의 계약을 지원합니다.

1. 비즈니스 지향적 인 SHARNELL 선형 논리를 기반으로 수학 공식으로 만 구성되도록 제안 된 "경량"(논리적) 스마트 계약. 선형 논리는 완벽하게 예측할 수 있으므로 잠재적 인 취약성을 최소화 할 수 있습니다.

논리적 스마트 계약은 조건 및 매개 변수를 포함하는 "데이터 카드"와 전체 또는 부분 성취 및 액츄 에이 팅 가능성을 고려하여 이러한 조건 및 매개 변수를 고려한 수식 자체로 구성됩니다. 논리적 계약의 각 조건은 데이터 카드에 배치되고 해당 기호가 지정되도록 제안됩니다.

나중에 계약 기간을 완전히 반영한 수식이 작성됩니다. π- 미적분 시스템은 계산을 병렬로 실행하는 데 사용됩니다.

이러한 유형의 현명한 계약은 multisig, escrow 등과 같은 가장 일반적인 작업과 트랜잭션을 수행하는 데 이상적입니다. 우리 시스템의 첫 번째 버전에서는 Petri Nets 를 기반으로 한 그래픽 편집기를 통해 제작할 것을 제안합니다.

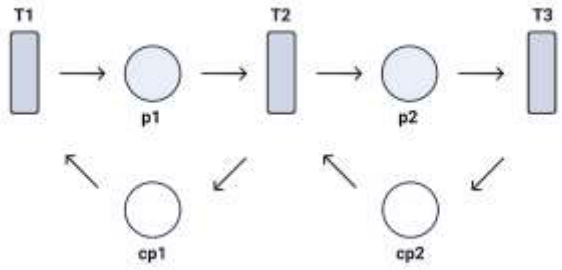

Figure 8. Smart contracts

2. "무거운"지능형 계약은 과학 계산 및 신경 네트워크 교육과 같은보다 복잡한 문제를 해결하기위한 코드를 포함하도록 제안되었습니다. 이들은 계산을위한 지불과 함께 시스템의 전용 지점에서 실행됩니다. 그러한 계산에 대한 지불은 ENQ 에서 사용자 정의 비율로 제공 될 것을 제안합니다. 또한 π- 미적분 시스템과 세션 유형이있는 채널 시스템을 사용할 것을 제안합니다.

4.6 티켓 및 마크

이전에 언급했듯이 Enecuum 은 "티켓"(해당되는 경우 "티켓", "티켓")의 개념을 지원하는 것을 목표로합니다. 티켓은 토큰과 유사한 암호 학적 대리 역할을하며 시스템의 모든 사용자가 만들 수 있습니다. 티켓은 ENQ 의 순환이 의도되지 않은 전용 분기를 만드는 데 사용됩니다. 티켓은 해당 분기에 대한 액세스 키와이 분기의 트랜잭션에 대한 암호 해독 키로 사용되며 Enecuum

사용자간에 자유롭게 전송할 수 있습니다.

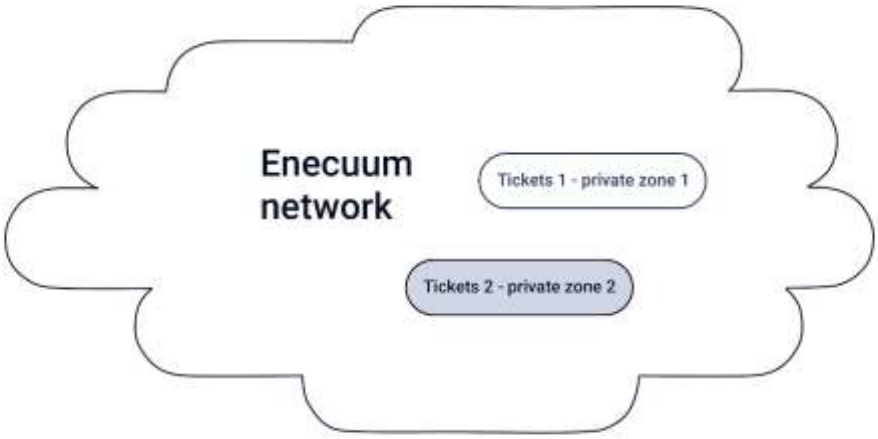

Figure 9. Tickets and Ticket branches
(Global ENQ network, Ticket branch #1, Ticket branch #2)

티켓은 해당 Ticket 지점에서 받아 들여지는 교환의 기본 매체가 될 수 있습니다. 이 토큰을 ENQ 로 변환하면 해당 티켓을 통해 발급됩니다.

Ticket 지점의 주요 목적은 기업과 고객간에 쉽게 상호 작용할 수 있도록 블록 체인 기반의 유연한 환경을 조성하는 것입니다.

"마크"는 Enecuum 의 기능을 확장하는 것을 목표로하는 또 다른 도구입니다 (해당되는 경우 "마크"또는 "마크"). 마크는 토큰, 거래 또는 지갑에 라벨을 붙이려고하며 별도의 단위로 존재하지는 않지만 지불 단위와 만 결합됩니다. 마크는 태그가 붙은 객체의 특정 기능을 나타내는 데 사용되며 규정 된 용어 나 특정 작업을 엄격하게 실행하는 데 사용됩니다. 표는 최종적이고 돌이킬 수없는 의도로 작성되었으며 변경할 수 없으며 작성하기 전에 결정됩니다.

Enecuum 은 다음 유형의 마크를 제공하는 것을 목표로합니다.

• 거래 촉진 마크는보다 빠른 거래를 촉진합니다.

• 증거금 통계표에 통계 축적에 자료가 축적되면 보상 표가 ENQ 로 변환됩니다 (4.3 참조).

• 토큰 라벨링 마크는 지불 단위에 사용자 정의 규칙 세트를 적용합니다 (예 : 표시된 단위에 적용할 수있는 작업 목록을 제한하고 해당 마크가있는 지갑에만 전송할 수 있음). 이 기능은 예산 관리, 구매 관리 및 직접 대출 관리 지원을 효과적으로 도와줍니다.

5. 문제 및 해결책

5.1. 확장 성

공개 블록 체인 시스템이 직면 한 가장 중요한 주제 중 하나는 많은 거래를 저렴하고 안전하게 진행하는 것입니다. 확장 성은이 기술의 세계적 규모 채택에 필수적입니다. Bitcoin 과 Ethereum 의 처리량은 종종 초당 50,000 건 이상의 처리가 가능한 VisaNet 시스템과 비교되며 [14] 가장 널리 사용되는 크립토 통화의 현재 처리량보다 수천 배나 더 큽니다. 전 세계적으로 엄청난 속도로 증가하는 cryptocurrency 사용자의 수를 감안할 때 현재 분산 시스템의 트랜잭션에 대한 피크 타임 비용은 엄청나게 높아질 수 있습니다.

우리는 블록 크기의 단순한 증가가 문제의 부분적이고 일시적인 해결책이라고 믿지만, 기본적인 확장 성 문제는 해결하지 못할 것입니다. 현재 블록의 데이터는 영구적으로 저장되며 블록 체인의 크기가 꾸준히 증가 할 것입니다. 처리량이 증가하면 크기도 더욱 빨라질 것입니다. 결과적으로 대기업 만이 방대한 데이터 세트를 저장하고 업데이트하기에 충분한 리소스를 할당 할 수있게되어 네트워크의 중앙 집중화를 이끌어 낼 수 있습니다.

HyperDAG (4.1 참조)를 사용하여 트랜잭션을 기록하고 저장하면 Enecuum 은 블록 체인을 별도의 지사 또는 지사의 일부로 제시되고 병렬 처리되는 샤딩 기술 구현에 이상적이라고 생각합니다. . 다양한 블록 크기의 샤딩을 결합한 Enecuum 은 시스템의 보안을 위태롭게하지 않으면 서 초당

수십 심지어 수십만 트랜잭션을 효율적으로 처리 할 수 있습니다. 대부분의 경우 거래 결과 커미션은 0 또는 최소가 될 것입니다.

또한 시스템에서 잠재적으로 무제한의 지사를 지원하므로 자체 Enchuum 지사에서 자체 블록 체인이나 더 많은 작업 부하가 필요없이 다양한 분산 비즈니스 애플리케이션을 생성 할 수 있습니다. 각 분기마다 서비스 별 요구 사항을 반영하도록 개별적으로 조정 된 사용자 지정 규칙 집합을 가질 수 있습니다. 또한 각 지사는 시스템의 모든 구성원에 대해 열거 나 참여자 목록이 정의 된 비공개로 제안 될 수 있습니다. 트랜잭션 속도 또는 블록 크기를 특정 분기에서 업그레이드해야하는 경우 자체 규칙을 수정하기 위해 노드를 도입 할 수있는 방법이 제안됩니다. 이 경우 유일한 제약은이 분기의 노드 용량입니다.

Enecuum 의 아키텍처는 잠재적 인 무제한 크기의 매크로 블록을 지원할 예정입니다.이 솔루션은 프로토콜이 최신 CPU 의 성능 향상과 동시에 확장 될 수 있도록 해줍니다.

5.2. 보안

낮은 지방 분권 문제

1 세대 블록 체인 시스템은 거래 확인을 위해 PoW 를 사용했습니다. PoW 는 DoS (Denial-of-Service) 및 스팸과 같은 다양한 유형의 공격으로부터 블록 체인 시스템을 보호하는 입증 된 효율성을 갖춘 신뢰할 수있는 알고리즘입니다. cryptocurrencies 의 인기와 가치가 증가함에 따라, PoW 광산은 광산 프로젝트에 투자 된 수억 달러의 대규모 사업으로 변모했습니다.

중국의 전력 및 노동 비용이 낮 으면 중국 대륙에 대규모 광산 채굴 집계가 이루어졌습니다. 이 상황은 광부의 대규모 풀과 잠재적 인 "51 % 공격"가능성 사이의 잠재적 인 결합으로 인해 관련 블록 체인 시스템 보안을 위험에 빠뜨립니다. ASIC 장치의 출현은 정기적 인 광산 굴착 장치를 사용하여 경제적 감각을 잃어 버렸고 대규모 투자자들에게보다 높은 수준의 채광 용량 중앙 집중화를 가져옴으로써 문제를 더욱 악화 시켰습니다 [16].

Enecuum 에서 세 가지 유형의 광업과 Cryptonight 암호화 프로토콜을 결합하면 지리적으로뿐만 아니라 다양한 장치 유형 및 인구 통계와 관련하여 시스템에서 고도의 분산화를 달성 할 수 있다고 믿어집니다. 우리는 이러한 기능이 Enecuum 을 가장 안전한 분산 레지스트리 중 하나로 만드는 데 도움이 될 것으로 믿습니다. 그 외에도, 블록 체인 상태 데이터를 수집하고 분석하는 시스템에

통계 분기 (4.3 참조)가 존재하면 Enecuum 과 그 사용자를 여러 유형의 잠재적 위협으로부터 더욱 안전하게 보호 할 것입니다. 모든 참가자들.

현명한 계약의 취약점

똑똑한 계약의 발명은 전체 cryptocurrency 산업에 강력한 추진력을 주었지만 현재까지 구현에는 많은 약점이 있습니다. 스마트 계약서가 블록 체인에 게시되면 수정할 수 없으므로 작성 과정에서 오류가 발생하여 사용자에게 수백만 달러의 손실을 줄 수 있습니다. 이는 다양한 암호 해독 프로젝트에서 한 번도 발생하지 않은 상황입니다 [16].

현명한 계약의 보안을 평가하는 기존의 방법은 주로 커뮤니티의 개발자가 수동 코드 감사로 진행합니다. 똑똑한 계약 생성 및 테스트 방법은 매우 비효율적이라고 주장됩니다. 특히 스마트 컨트랙트가 생성되는 속도가 현저히 빨라지고 복잡성이 증가한다는 점을 고려할 때 똑똑한 계약을위한 가장 인기있는 플랫폼 인 Ethereum 은 개발자 커뮤니티에서 아직 인기를 얻지 못하고있는 특정 프로그래밍 언어 인 Solidity [17]로 작성하려고합니다. 숙련 된 Solidity 개발자가 급격히 부족하여 문제를 완화하지는 못합니다.

SHARNELL Smart Contracts 의 구현에 사용하도록 제안 된 선형 논리는이 기술의 보안을 새로운 차원으로 끌어 올리는 것을 목표로합니다. 그것은 모든 스마트 계약이 블록 체인에 게시되기 전에 신뢰성있는 자동 테스트를 도입 할 것을 제안합니다. 이것은 차례로 오류 및 잠재적 취약성의 가능성을 최소화하는 것을 목표로합니다.

또한, SHARNELL Smart Contracts 의 제안 된 언어는 가장 인기있는 스크립팅 프로그래밍 언어 중 하나 인 JavaScript 이므로 많은 전문가가 SHARNELL 스마트 계약 생성에 참여할 기회를 가지며 이는 비용 절감을 제안합니다. 똑똑한 계약 개발.

블록 체인을 통한 전력 집중화

Bitcoin 네트워크의 실패한 Segwit2x 업그레이드와 Bitcoin Cash 를 생성 한 하드 포크는 커뮤니티에서 잠재적 인 불일치를 강조합니다 [18]. 불행하게도, Bitcoin 의 아키텍처는 광부, 개발자 및 일반 사용자가 프로토콜에 대한 제안 된 변경 사항에 대한 견해를 형성하는 다양한 동기를 가지고있는 방식으로 배열됩니다 [2]. 경쟁 이익은 변화하는 시장 상황에 대한 적응을 늦추는 효과가 있습니다. 해결되지 않으면 시스템 노후화로 이어질 수 있습니다.

Enecuum 은 매개 변수 또는 새로운 변경 사항에 대한 사용자의 제안을 온 체인 투표 (on-chain vote)하여 플랫폼 개선 프로세스에 영향을 줄 수있는보다 공정한 기회를 사용자에게 제공함으로써이 문제를 해결하려고합니다. 또한 주 시스템 브랜치에서 릴리스되기 전에 보조 브랜치 중 하나에서 잠재적 인 실패를 테스트 할 수 있으므로 변경 사항 구현시 안전한 프로세스가 필요합니다.

5.3. 은둔

Cryptocurrencies 는 익명 성을 가지고 있으므로 불법 활동을위한 충분한 기회를 제공한다는 것이 일반적인 믿음입니다. 네트워크 내의 모든 트랜잭션이 투명하고 공개되어 있다는 사실에도 불구하고 그 뒤에있는 실제 개인과 회사는 알 수 없다는 것이 일반적인 믿음입니다. 그러나 열린 블록 체인의 모든 작업은 디지털 추적을 영원히 유지하므로이 추적에서 수행 된 상세한 분석은 높은 정확도로 실제 거래 상대방을 파악하는 데 도움이 될 수 있기 때문에 완전히 사실이 아닙니다. 따라서 침입자가 공개 주소를 실제 사람이나 회사와 일치 시키면 중요한 기밀 데이터에 액세스하여 돌이킬 수없는 손해를 입힐 수 있습니다 [15] [19].

티켓 지점 (4.3 참조)은 Enecuum 사용자에게 개인 정보 유출의 위험을 최소화하는 개인 모드로 거래를 수행하는 수단을 제공합니다. 티켓은 지사에서 트랜잭션을 암호화하는 핵심 키이므로 티켓 보유자 만이 지니고있는 트랜잭션의 세부 사항을 볼 수 있습니다. 티켓 지점은 특정 지점 (Ticket 지점)에서 특정 토큰을 발행 할 수 있도록 제안합니다. 그러한 토큰을 Enecuum 교환의 주요 매체 인 ENQ 와 교환해야하는 경우 티켓은 교환을 수행하는 데 중요한 역할을합니다. 이렇게하면 티켓이 트랜잭션을 안전하게 보호하는 암호화 키 역할을합니다.

외부의 관심에서 티켓 지점 내부, 그러한 거래를 확인하기 위해 전체 네트워크의 용량을 사용하는 동안 빠른 속도를 보장하고자합니다.

6. 사용 사례

6.1 초기 코인 제공 플랫폼

제안 된 Enecuum 블록 체인의 높은 처리량은 신생 기업이 네트워크 중단 위험없이 모든 규모로 자금을 조달 할 수 있도록 지원합니다. 따라서 초기 동전 제공 업체 (ICO) 참가자는 ICO 에 참여하고 토큰을 신속하게받을 수 있음을 확신 할 수 있습니다. Enecuum 의 현명한 계약이 JavaScript 로 구현되도록 제안 되었기 때문에 모든 웹 개발자에게 쓰기 쉽기 때문에 작성 비용이 크게 줄어들 것입니다. 또한 선형 논리를 사용하면 스마트 계약 코드의 잠재적 취약성을 제거하고 해킹의 위험을 최소화하는 데 도움이됩니다.

"취소 모델"을 통해 발급자는 복잡한 ICO 를 단계별로 진행하고 참가자 중 어떤 단계에서든 자금을 반환 할 수 있습니다. 시스템 고유의 토큰 표기법은 ERC-20 표기법과 유사하게 Enecuum 기반으로 작성된 토큰을 ICO 이후에 암호 교환 서비스로 간단하게 입력하기위한 것입니다.

토큰 발급자는 토큰 사용 사례를 적절하게 디자인하고 해당 토큰이 적용 가능한 모든 법적 및 규제 의무를 준수하도록해야합니다.

6.2 금융 서비스 및 지불 인프라

Enecuum 의 Tickets and Marks 를 사용하여 은행, 정부 기관 및 거래 조직이 신용 및 예산 자금의 목표 지출을 안정적으로 관리 할 수 있도록하는 것이 우리의 목표입니다. Enecuum 인프라는 또한 안전하고 효율적인 지불을 위해 활용 될 수 있습니다.

예를 들어, 은행은 고객의 데이터베이스를 가질 수 있으며, 비즈니스의 성격 (건설 회사, 산업 장비 공급 업체 등)에 따라 분류됩니다. 은행은 고객에게 구체적이고 뚜렷한 표시가있는 토큰에 대해 직접 대출을 할 수 있습니다. 고객은이 토큰을 사용하여 사전 정의 된 특정 조직에게만 지불하고 발급 된 대출 목적에 따라 지출 할 수 있습니다.

또한 트랜잭션에 주석을 추가 할 가능성은 예를 들어 각 고객의 기록을 유지하는 블록 체인 기반 보험 서비스를 허용 할 수 있습니다. 이 서비스는 현명한 계약을 통해 자동 계산을 수행하여 각 사용자의 보험 보상 범위와 관련된 정보를 블록 체인에 직접 보관하고 저장할 수 있습니다.

6.3 분산 계산

Enecuum 은 전용 지사에서 "무거운"스마트 계약을 실행할 수있는 능력을 목표로합니다. 또한 Enecuum 은 주요 Enecuum 브랜치 (신경 네트워크 교육, 과학 계산, 컴퓨터 그래픽 렌더링, JS 라이브러리 등에 유용함)에서 작업량을 증가시키지 않으면 서 높은 계산 능력을 요구하는 복잡한 계산을 허용하는 것을 목표로합니다. Ethereum 블록 체인의 거래 가격 개념과 유사하게 ENQ 에서 유연한 비율로 의도 된 "무거운"스마트 계약을 사용하기위한 지불. 계산을 수행하라는 요청을 작성하여 고객은 가격을 설정하고 광부는 작업에 대한 계산 능력을 제공하는 것이 유익한 지 여부를 결정합니다. 광부가 조건에 동의하는 경우, 고객의 자금은 스마트 계약에 의해 향후 지불을 위해 예약됩니다. 과제가 완료되고 유효한 결과가 제공되면 자금이 방출되어 자동으로 광부에게 양도됩니다.

6.4 분산 스토리지

샤딩 기술을 적용하고 트랜잭션 복제 매개 변수를 변경할 수 있으므로 사용자의 장치에서 디스크 공간을 효과적으로 사용할 수 있습니다. 예를 들어, 4 명의 사용자가 각각 5GB 의 공간을 제공하고 복제 및 샤딩 매개 변수가 50 %로 설정된 경우 파일의 유효 저장 용량은 10GB 입니다. 전체

네트워크에이 패턴을 외삽 해보면, "글로벌 분산 형 디스크"의 크기는 데이터의 가용성과 충분한 액세스 속도를 유지하면서 비례하여 증가 할 것입니다. 이것은 사용자가 미래에 Enecuum Blockchain 위에 분산 형 호스팅, 클라우드 데이터 스토리지 서비스 및 컨텐트 전달 네트워크와 같은 서비스를 구축 할 수 있음을 의미합니다.

다시 말하지만, SHARNELL Smart Contracts 및 Ticket 을 이러한 데이터 브랜치 상단의 암호화 키로 적용하면 사용자는 토큰으로 지불 된 분산 된 (불변) 컨텐츠로 복잡한 유료 액세스 서비스를 작성할 수 있습니다.

6.5 소액 결제 및 IoT 애플리케이션

Enecuum 시스템의 작업량은 Eneecuum 사용자 수가 증가함에 따라 증가 할 것이고 분산 된 응용 프로그램은 Enecuum 블록 체인 위에 개발 될 것입니다. 그러나 Enecuum 은 자체 컨센서스 룰 세트를 사용하여 별도의 블록 체인 분기를 만들 수 있도록하여 메인 시스템에서 작업 부하를 제거합니다. 이것은 차례로 광부의 활동을 자극하고 소액 거래 서비스 구현에 유익한 조건을 조성하고자합니다.

Enecuum 은 분산 된 소액 거래 서비스에 대해 제로 거래 수수료를 제안하고 단일 지갑에서 많은 소액 거래를 포함하는 중앙 소액 거래 서비스의 경우 거래 당 매우 낮은 수수료를 제안합니다. 예를 들어, 매일 10,000,000 개의 트랜잭션을 각각 10MB 의 대형 매크로 블록에 쉽게 기록 할 수 있습니다. 수수료는 블록 당 계산되므로 거래 당 매우 낮은 수수료가 제안됩니다.

우리는 이것이 "사물의 인터넷"과 관련하여 Enecuum 의 기능을 완벽하게 사용한다고 믿습니다. 다양한 장치에서 PoA 마이닝을위한 간단한 클라이언트를 구현하면 운반 된 거래 수수료를 완전히 충당 할 수 있습니다. 게다가, Enecuum 네트워크 프로토콜은 그 사이에 메쉬 네트워크를 구축함으로써 그러한 장치의 높은 가용성을 제공하도록 설계되었습니다.