V1.00

Paragon Pay

실물 경제와 블록체인의 연결

WHITEPAPER

Paragon Pay

00 Summary

마일리지 (Mileage)란, 고정 고객 확보를 위한 기업의 판매 촉진 프로그램으로써, 해당 기업을 이용하는 고객들이 이용 실적에 따라 점수를 획득할 수 있는데, 여기서 누적된 점수는 화폐의 기능을 합니다. 최초 항공사에서 시작되어 최근에는 신용 카드사, 통신 회사 등 고객 유치의 일환으로 이용하고 있는 마케팅 방식 중 하나입니다. 이러한 마일리지 포인트 산업을 통하여 경쟁이 치열해지고 있는 상황에서, 많은 기업들이 고객 애호도 및 활용성을 높이고, 구매 유인 수단으로 활용하기 위하여 대기업 및 일반적인 소상공인 업체들 또한 해당 방식을 활용하고 있습니다. 그만큼 마일리지 프로그램을 활용한 마케팅 촉진이 사업의 매출에 미치는 영향이 크다는 연구 결과 또한 발표되었습니다. 경쟁이 치열한 사업일수록, 고객으로 하여금 특정 기업이나 브랜드에 대하여 지속적인 사용 및 구매를 유도하고, 사용자들이 해당 브랜드에 대한 호의적인 이미지를 심는 등, 기업의 매출에 효과적이면서도, 고객에게 편익을 제공하는 면에서 마일리지 포인트 산업은 꾸준한 성장세로 나아가고 있습니다.

하지만, 이러한 마일리지 포인트 산업이 고객에게 제품 구매와 동시에 그 혜택을 제공하는 것이 아닌, 향후 일정 기간 동안 정해진 포인트를 적립하고, 권리를 행사하는 구조라는 점을 이용하여, 일부 기업에서는 마일리지를 사용하는 과정에서 초기 조건들이 불리하게 변경되거나 까다로워지는 경우가 발생하고 있어 피해사례가 증가하고 있는 상황입니다. 마일리지 사용 과정에 소비자가 피해를 발생하는 사례가 꾸준하게 증가될 경우, 기업은 해당 브랜드에 대하여 장기적이고 지속적인 고객 관계의 유지라는 기업과 소비자의 관계를 단절시키고, 소비자가 비호의적인 기업 이미지를 형성할 수밖에 없는 상황이 만들어집니다.

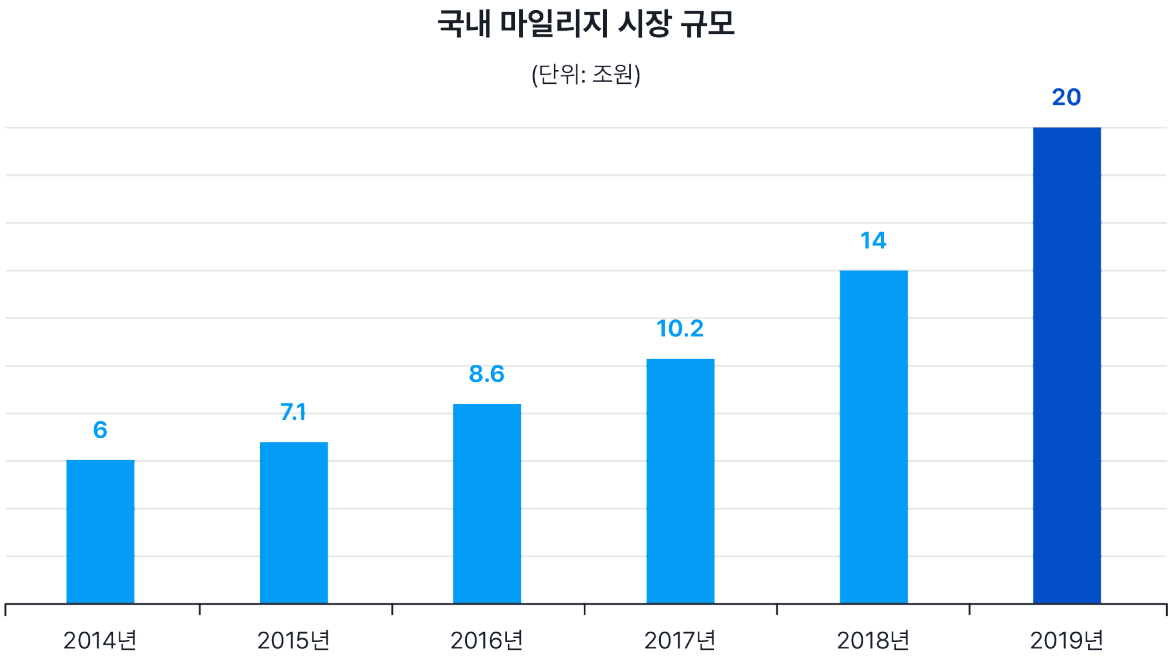
이에 Paragon Pay는 이러한 현상을 해결하기 위하여, 기존의 마일리지 포인트 산업의 문제점을 해결하고, 독자적인 연구 개발을 통하여 완성된 플랫폼을 제공하여 Paragon Pay 생태계 내 다양한 활용 방안을 제시하고자 합니다. 생태계 참여자는 Paragon Pay의 플랫폼을 활용하여 기존 낭비되거나 활용되지 못하던 마일리지 포인트를 블록체인을 활용한 플랫폼을 통해 안전하고 신뢰할 수 있는 사용 환경을 제공합니다. Paragon Pay는 향후 다양한 실물 경제의 산업 및 마일리지 포인트 관련 사업체들과 연계하여 기술 협업 및 사업 확장을 통하여 Paragon Pay의 글로벌 역량을 키워나가는 것을 목표로 하고자 합니다.

Paragon Pay

01 Market Trend

마일리지 포인트 사업은 2000년대 초반부터 인터넷이 일반에게 보급되면서 대중화가 진행되었고, 항공사, 카드사, 통신사, 이커머스 마켓을 주축으로 광범위한 분야에서 마일리지 포인트가 사용되고 있습니다. 2019년 기준으로 국내 포인트 시장은 약 20조 원, 글로벌 시장의 경우에는 약 200조 원의 규모로 추정되고 있습니다. 이는 2014년 국내 시장 규모가 6조 원이였던 점을 감안한다면, 시장의 확장 속도가 가파르게 성장하고 있다는 것을 알 수 있습니다.

마일리지 포인트 시장이 확대됨에 따라 더 많은 종류의 포인트 혜택들이 나오고 있는 상황으로 특히, 쇼핑몰의 경우에는 포인트를 운영하지 않는 곳을 찾기가 더 힘들 정도로 마일리지 포인트 제도가 보편화된 상황입니다.



출처: 통계청, 한국 소비자원

이러한 시장 확대의 이유로는 다양한 도메인의 플레이어들이 경쟁사와의 차별성을 위하여 각자의 플랫폼을 통하여 독자적인 마일리지 포인트를 발행하는 점을 중점으로, 소비 시장이 오프라인에서 온라인 시장으로 이동하며 세분화되어 가는 점에서 경제적, 기술적인 허들이 낮아짐에 따라, 시장에서도 마일리지 포인트 제도가 선택이 아닌 필수로 자리 잡고 있어 현재와 같은 성장세를 보여주고 있습니다.

02 Problem

마일리지 포인트 사업에서 발생할 수 있는 다양한 문제점들을 짚어보면, 마일리지 적립 누락, 사용 불가 등의 이유들을 볼 수 있습니다. 누락의 경우 후속 조치를 통하여 해결이 가능하여 비교적 사용자들의 불만이 적은 편이지만, 마일리지의 사용 제한은 기업의 정책이나 제도적인 방안이 마련되지 않는 이상 소비자의 불만이 높아질 수밖에 없는 상황입니다. 마일리지를 활용하고 사용하고자 하는 사용자들이 늘어나는 것에 비하여, 마일리지에 대하여 기업의 수익을 감소하는 것을 방지하기 위하여 마일리지 포인트의 사용 방식을 한정적으로 제한시키는 등의 정책 변경들로 인하여 사용자들은 꾸준히 모아둔 마일리지를 제대로 활용하지 못한다는 단점이 발생하게 됩니다. 이는 결과적으로 마일리지 포인트 프로그램의 최대 강점인 지속적인 고객 관계를 통한 브랜딩 이미지를 오히려 악화시키고, 소비자들의 이탈로 이어질 수 있습니다.

상기했던 내용처럼 마일리지 포인트 시스템을 활용하는 기업들이 점진적으로 증가하고 있으나, 오히려 이런 흐름이 사용자들에게는 혼선을 주고 있습니다. 법적으로 재량 사항으로 규정되고 있는 마일리지 포인트는 정확한 기준점이 없이 업종별로 상이한 마일리지 포인트 정책을 제시하고 있어, 적립에 대한 비율, 사용 방식, 기간 등이 상이하며, 같은 업종이라고 한들 브랜드가 달라 보유하고 있는 포인트를 적재적소에 활용하기가 힘든 상황입니다. 또한 해당 브랜드가 마일리지 포인트 사업의 종료나 폐업 등을 진행하게 될 경우, 사용자는 의도치 않게 자신이 보유하고 있는 마일리지가 소멸되는 상황이 발생합니다.

또한 재량 사항으로 진행되다 보니, 마일리지 포인트 사용에 대한 정책들을 기업 내에서 언제든지 임의적으로 변경할 수 있어, 소비자의 기대 가능성을 저해하고 있는 상황입니다. 이는 수익을 추구하는 것이 목적인 기업에서 마일리지를 소비자에게 일방적으로 부여하는 하나의 보너스 개념으로 간주하고 있기에 발생할 수 있는 사항으로, 사용자들의 의견과는 관계없이 이러한 기업이 선택한 정책의 흐름에 따를 수밖에 없습니다.

03 Paragon Pay

Paragon Pay에서는 마일리지 서비스를 블록체인 기술과 결합한 플랫폼을 구축하고, 독자적인 보안 기술을 적용한 솔루션 제공함으로써 현재 마일리지 서비스 시장에서 문제점으로 지적되는 사항들을 해결하는 새로운 대안을 제시한 것을 목표로 합니다. Paragon Pay는 기축 토큰인 PARAGON을 활용하여 플랫폼 생태계에 참여할 수 있도록 개발되었습니다. Paragon Pay 플랫폼을 통하여 흩어져 있던 마일리지를 통합하고, 사용자는 PARAGON을 활용하여 다양한 서비스를 활용할 수 있으며, 더 나은 정책들을 통하여 차세대 마일리지 활용 방식을 제공함을 목표로, 플랫폼 생태계에 참여한 유저들에게 다양한 혜택을 제공하는 차세대 플랫폼으로 자리 잡고자 합니다. Paragon Pay는 다양한 서비스 제공 방향성과 사업 영역의 확장을 위하여 향후 다양한 관련 업체 및 플랫폼과의 파트너십, 협업 등의 사업 영역을 확장해 나갈 예정입니다.

Why Blockchain?

블록체인이란 다수의 거래 내역을 묶어 블록을 구성하고, 해시를 이용하여 여러 블록들을 체인처럼 연결한 뒤, 다수의 사람들이 복사하여 분산 저장하는 알고리즘을 의미합니다. 블록체인 기술을 이용하면 데이터의 위변조가 불가능하여 권위 있는 중개 기관이 없더라도 신뢰할 수 있는 안전한 거래와 데이터를 처리할 수 있습니다.

블록체인은 은행 등 제3의 중개 기관이 없더라도 블록체인 기술을 이용하면 누구나 신뢰할 수 있는 안전한 거래를 할 수 있습니다. 블록체인은 암호 화폐뿐 아니라, 온라인 거래 내역이 있고 이력 관리가 필요한 모든 데이터 처리에 활용할 수 있습니다. 블록체인 기반의 Smart Contract, 물류 관리 시스템, 문서 관리 시스템, 의료 정보 관리 시스템, 저작권 관리 시스템, 소셜 미디어 관리 시스템 등 다양한 활용이 가능하며, 4차 산업 혁명의 핵심 기술 중 하나입니다. 중개기관이 필요 없는 블록체인 기술을 통하여 인류는 새로운 거래 방식과 조직 운영 원리를 바탕으로 사회적 변화와 혜택을 누릴 수 있을 것으로 기대심리가 올라가고 있는 상황입니다. 또한 블록체인을 활용함으로써 다음과 같은 이점을 제공합니다.

Reliability (신뢰성)

모든 종류의 정보를 블록체인에 기록하고 안전하게 저장하여 신뢰를 구축합니다

Efficiency (효율성)

복잡한 디지털 거래, 상세한 제품 정보 기록, 저장 및 추적을 통해 관련 정보에 액세스 합니다.

Transparency (투명성)

수학적 암호화 알고리즘을 사용하여 다양한 유형의 정보를 코드로 변환하여 수많은 기록이 컴퓨터에 기록됩니다

Security (보안)

블록체인에서 거래 정보 및 사용자 개인 정보를 보호합니다.

Way to Paragon Pay

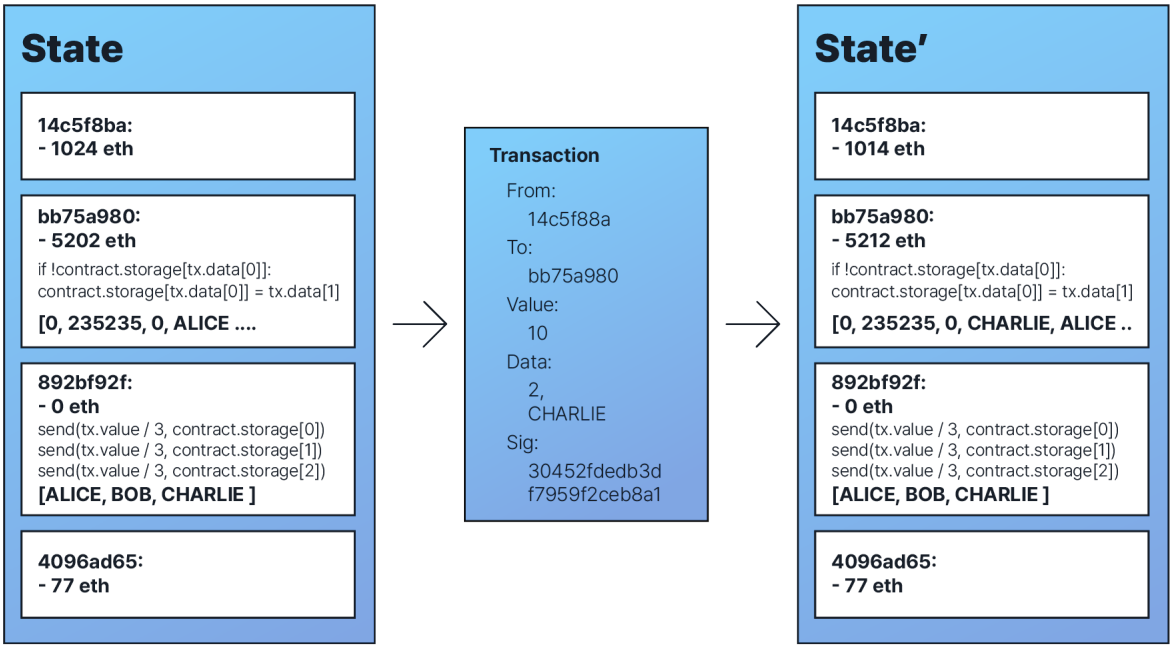
[해당 사항은 사업의 진행 방향성에 따라 변경될 수 있습니다.]

Paragon Pay는 자체적인 기술력으로 개발된 어플리케이션을 통하여 생태계에 참여할 수 있습니다. Paragon Pay는 암호 화폐가 실생활에 활용성이 떨어진다는 문제점을 해결하고, 실생활에 활용 가능한 실물 경제 연계 플랫폼입니다. Paragon Pay는 자체적으로 개발된 어플리케이션의 Marketplace에서 카카오톡 선물하기 시스템을 기반으로 카카오톡의 주력 상품들을 판매할 뿐만 아니라 향후 주유, 레저, 숙박과 같은 다양한 분야의 오프라인 가맹점들과 연계를 하여, PARAGON의 활용 영역을 늘려나갈 예정입니다. 또한 Paragon Pay 생태계 참여한 유저들을 위해 기존 플랫폼들 이상의 보상 체계 및 정책을 준비 중이며, 장기적인 생태계 참여자들을 위한 보상으로써, 일정 기간, 일정 수량 이상의 PARAGON을 보유할 경우, 0.5~5%의 추가적인 할인 혜택을 제공받을 수 있는 멤버십 혜택을 제공할 예정입니다.

Technology

Paragon Pay는 이더리움 블록체인 네트워크에서 정한 표준 토큰 프로토콜인 ERC-20 기반으로 개발되었습니다. Paragon Pay는 자체적인 블록체인을 기반으로 다양한 탈중앙화를 목표로 개발된 어플리케이션이 작동할 수 있도록 고안된 플랫폼 네트워크입니다. 이더리움 플랫폼은 튜링 완전 언어를 내장하고 있는 블록체인으로서, 필수적이고 근본적인 기반을 제공하며, Smart Contract를 활용하여 쉽고 빠른 블록체인 트랜잭션을 활용할 수 있으며, 이더리움 생태계의 호환 및 사용이 가능합니다.

ERC-20의 Smart Contract는 블록체인 기반으로 금융거래, 부동산 계약, 공증 등 다양한 형태의 계약을 체결하고 이행하는 것을 말하며, 코드에 적힌 계약 조건이 만족되면 그 즉시 계약이 성사됩니다. 이때 계약 상대방이 신뢰할 수 있는지, 중간에 보증할 수 있는 제3자가 필요한지, 계약이 안전하게 진행되는지 등에 대한 고민이 필요하지 않으며 자동으로 처리가 진행됩니다. 어떠한 다운 타임, 검열, 사기행위, 제3자 간섭 없이 프로그래밍된 대로 정확 실행되는 프로그램으로써 블록체인에 기록되기 때문에 누구도 처음에 명시된 조건을 바꿀 수 없습니다.



이는 이더리움 상태 변환 함수를 통해서 진행되며, APPLY(S, TX) -> S'는 다음처럼 정의될 수 있습니다. 트랜잭션의 형식에 제대로 맞는지, 올바른 개수 값을 가지고 있는지에 대하여 체크하고, 서명이 유효한지, 논스가 발신처 어카운트의 논스와 일치하는지를 체크합니다. 그렇지 않다면 오류를 반환하게 됩니다. STARTGAS * GASPRICE로 트랜잭션 수수료를 계산하고, 서명으로부터 발신처 주소를 결정합니다. 발신처 어카운트 잔고에서 이 수수료를 제하고 발신자 논스를 증가시킵니다. 발신처 장고가 충분하지 않으면 오류를 반환하며, GAS = STARTGAS로 초기화한 후, 트랜잭션에서 사용된 바이트에 대한 값을 지불하기 위하여, 바이트당 gas의 특정 수량을 차감하게 됩니다. 발신처 어카운트에서 수신처 어카운트로 트랜잭션 값을 보냅니다. 수신처 어카운트가 존재하지 않으면 새로 생성하게 되며, 수신처 어카운트가 Contract 일 경우, Contract 코드를 끝까지, 또는 gas가 모두 소모될 때까지 수행하게 됩니다. 발신처가 충분한 수수료를 가지고 있지 못하여 값 전송이 실패하거나, 코드 수행 시 gas가 부족하면, 모든 상태 변경을 원상태로 돌려놓습니다. 단 수수료 지불은 제외되며, 이 수수료는 채굴자 어카운트에 더해지게 됩니다. 이 외에 모든 남아있는 gas에 대한 수수료를 발신처에 돌려주고, 소모된 gas를 지불된 수수료를 채굴자에게 보내는 구조로 진행됩니다. 예를 들어 다음과 같은 컨트렉트 코드를 가정해 보겠습니다.

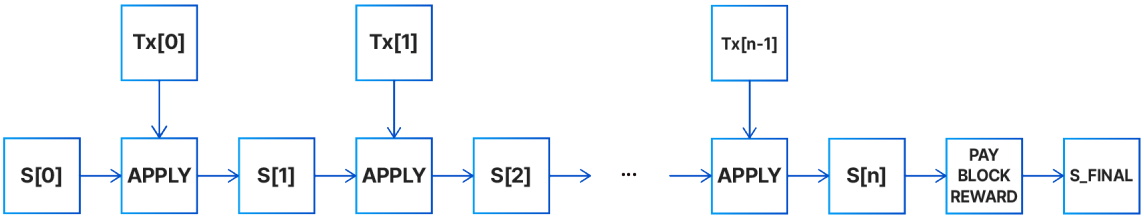
```
if !self.storage[calldataload(0)]:
    self.storage[calldataload(0)] = calldataload(32)
```

실제로 Contract 코드는 로우-레벨 EVM 코드로 작성되나, 이 예제는 이해하기 쉽게 하기 위해, 이더리움 하이-레벨 언어 중 하나인 Serpent를 예시로 하였습니다. 이 코드는 EVM 코드로 컴파일될 수 있습니다. Contract의 스토리지는 비어있다고 가정하고, 트랜잭션이 10 ether, 2000 gas, 0.001 ether gasprice, 64 바이트의 데이터(0-31 바이트까지는 숫자 2를 나타내고, 32-63 바이트는 CHARLIE라는 문자열)를 보낸다고 가정할 경우 이 경우 상태 변환 함수의 프로세스는 다음과 같습니다.

- 트랜잭션이 유효하고 형식에 제대로 맞는지 확인한다.
- 트랜잭션 발송처가 최소 2000 * 0.001 = 2 ether를 가지고 있는지 확인하고, 그럴 경우, 발송처의 어카운트에서 2 ether를 뺀다.
- gas = 2000으로 초기화한 후, 트랜잭션은 170바이트 길이를 가지고, 바이트당 수수료는 5라고 가정하면, 850을 빼야 하고 결국 1150 gas가 남게 된다.
- 발송처 어카운트에서 추가 10 ether를 빼고 이것을 Contract 어카운트에 더한다.
- 코드를 실행시킨다. 이 경우는 간단한데, Contract의 index 2에 해당하는 스토리지가 사용되었는지 확인하고 (이 경우, 사용되지 않았다.) index 2에 해당하는 스토리지 값을 CHARLIE로 설정한다. 이 작업에 187 gas가 소비됐다고 가정하면, 남아있는 gas의 양은 1150 - 187 = 963 이 된다.
- 963*0.001 = 0.963 ether를 송신처의 어카운트로 되돌려주고, 결과 상태를 반환한다.

트랜잭션의 수신처에 Contract가 없으면, 총 트랜잭션 수수료는 제공된 GASPRICE와 트랜잭션의 바이트 수를 곱한 값과 같아지고, 트랜잭션과 함께 보내진 데이터는 관련이 없어지게 됩니다. 메시지는 트랜잭션과 마찬가지 방식으로, 상태를 원래 상태로 되돌린다는 것에 주목해야 하며, 메시지 실행 시 gas가 부족하게 되면, 그 메시지 실행과 그 실행에 의해 촉발된 다른 모든 실행들은 원래대로 되돌려지게 되지만, 그 부모 실행은 되돌려질 필요가 없습니다. 이는 Contract가 다른 Contract를 호출하는 것은 안전하다는 것을 의미합니다. A가 G gas를 가지고 B를 호출하면, A의 실행은 최대 G gas만을 잃는다는 것을 보장받게 됩니다. Contract를 생성하는 CREATE라는 opcode를 보면, 실행 방식은 대체로 CALL과 유사하나, 실행 결과는 새로 생성된 Contract의 코드를 결정한다는 차이가 있습니다.

이를 통해 Paragon Pay 블록 안에 거래 기록뿐만 아니라 조건문과 반복 명령어 등 실행 코드를 포함하는 것이 가능하여 결제만 가능한 것이 아니라 다양한 서비스에서 사용할 수 있습니다. 이를 통한 이더리움 네트워크상에서 유통할 수 있는 토큰의 호환성을 보장하기 위해 개발되었으며, 온라인 환경에서 트랜잭션 진행 시 일정 행동이 불가역적으로 전개되는 Smart Contract를 통해 중앙 관리가 배제된 서비스 구현이 가능합니다. P2P 네트워크 상에서 거래 이력을 블록체인에 기록하는 한편 Smart Contract이나 실행 이력도 기록되며, 중앙 서버가 없는데도 네트워크 내 다른 노드들을 쉽게 찾을 수 있는 프로토콜을 통하여 부트 스트랩을 통한 일정 기간 동안 연결했던 모든 노드 목록을 유지합니다. 피어가 Paragon Pay 네트워크에 접속될 때, 마지막으로 지정된 시간 이내에 연결된 피어의 목록을 공유하는 부트 스트랩 노드에 먼저 연결되는 형식으로 다른 피어들과 연결되어 동기화되며, 메시지 확산을 위한 스웜, 통신을 위한 위스퍼, 트랜잭션과 블록 해시의 커뮤니케이션을 위한 ETH 프로토콜을 통해 P2P 커뮤니케이션을 블록체인상에서 실행하는데 가장 효율적인 방안으로 설계되었습니다.



Paragon Pay의 블록체인 프로토콜의 핵심인 이더리움 블록체인은 여러 면에서 비트코인 블록체인과 유사하나, 어느 정도 차이점들이 존재합니다. 이더리움과 비트코인에서의 각 블록체인 구조에 대한 주요 차이점으로는 비트코인과는 달리 이더리움 블록은 트랜잭션 리스트와 가장 최근의 상태(state) 복사본을 가지고 있다는 것입니다. 그것 외에도, 두 개의 다른 값 - 블록 넘버와 difficulty - 이 또한 블록 내에 저장됩니다.

기본적인 이더리움 블록 검증 알고리즘은 다음과 같습니다.

- 참조하고 있는 이전 블록이 존재하는지 그리고, 유효한지 확인한다.
- 현재 블록의 타임스탬프가 참조하고 있는 이전 블록의 그것보다 크면서, 동시에 현시점을 기준으로 15분 후보다 작은 값인지 확인한다.
- 블록 넘버, difficulty, 트랜잭션 루트, 삼촌 루트, gas 리미트 등(기타 다양한 이더리움 로우 레벨 개념)이 유효한지 확인한다.
- 블록에 포함된 작업 증명이 유효한지 확인한다.
- S[0] 이 이전 블록의 마지막 상태(state)라고 가정 하자.
- TX를 현재 블록의 n개의 트랜잭션 리스트라고 하자. 0부터 n-1에 대해, S[i+1] = APPLY(S[i], TX[i])로 설정하자. 어플리케이션이 오류를 반환하거나, 이 시점까지 블록에서 소모된 총 gas가 GASLIMIT를 초과하면 오류를 반환한다.
- 채굴자에게 지불된 보상 블록을 S[n] 덧붙인 후 이것을 S_FINAL이라 칭한다.
- 상태 S_FINAL의 머클 트리 루트가 블록 헤더가 가지고 있는 최종 상태 루트와 같은지를 검증한다. 이 값이 같으면 그 블록은 유효한 블록이며, 다르면 유효하지 않은 것으로 판단한다.

이러한 접근은 언뜻, 모든 상태를 각 블록에 저장할 필요성 때문에 매우 비효율적인 것처럼 보이지만, 실제로는 효율성의 측면에서는 비트코인과 비교됩니다. 그 이유로는 상태가 트리 구조로 저장되고, 모든 블록 후에 단지 트리의 작은 부분만이 변경되기 때문입니다. 보통, 인접한 두 개의 블록 간에는 트리의 대부분의 내용이 같고, 따라서 한번 데이터가 저장되면 포인터(서브 트리의 해쉬)를 사용하여 참조될 수 있습니다.

패트리시아 트리(Patricia tree)로 알려진 이러한 종류의 특별한 트리는 머클 트리 개념을 수정하여 노드를 단지 수정할 뿐만 아니라, 효율적으로 삽입되거나 삭제하여 이러한 작업을 수행할 수 있도록 해줍니다. 또한, 모든 상태 정보가 마지막 블록에 포함되어 있기 때문에, 전체 블록체인 히스토리를 모두 저장할 필요가 없어지게 됩니다. 이 방법을 비트코인에 적용한다면 5~20배의 저장 공간 절약의 효과가 생기게 됩니다. 물리적인 하드웨어 관점에서 볼 때, Contract 코드는 "어디에서" 실행되는가 하는 의문이 쉽게 들 수 있습니다. 간단한 해답은 다음과 같습니다. Contract 코드를 실행하는 프로세스는 상태 전환 함수 정의의 한 부분이고, 이것은 블록 검증 알고리즘의 부분입니다. 따라서, 트랜잭션이 블록 B에 포함되면 그 트랜잭션에 의해 발생할 코드의 실행은 현재 또는 향후에 블록 B를 다운로드하고 검증하는 모든 노드들에 의해 실행됩니다.

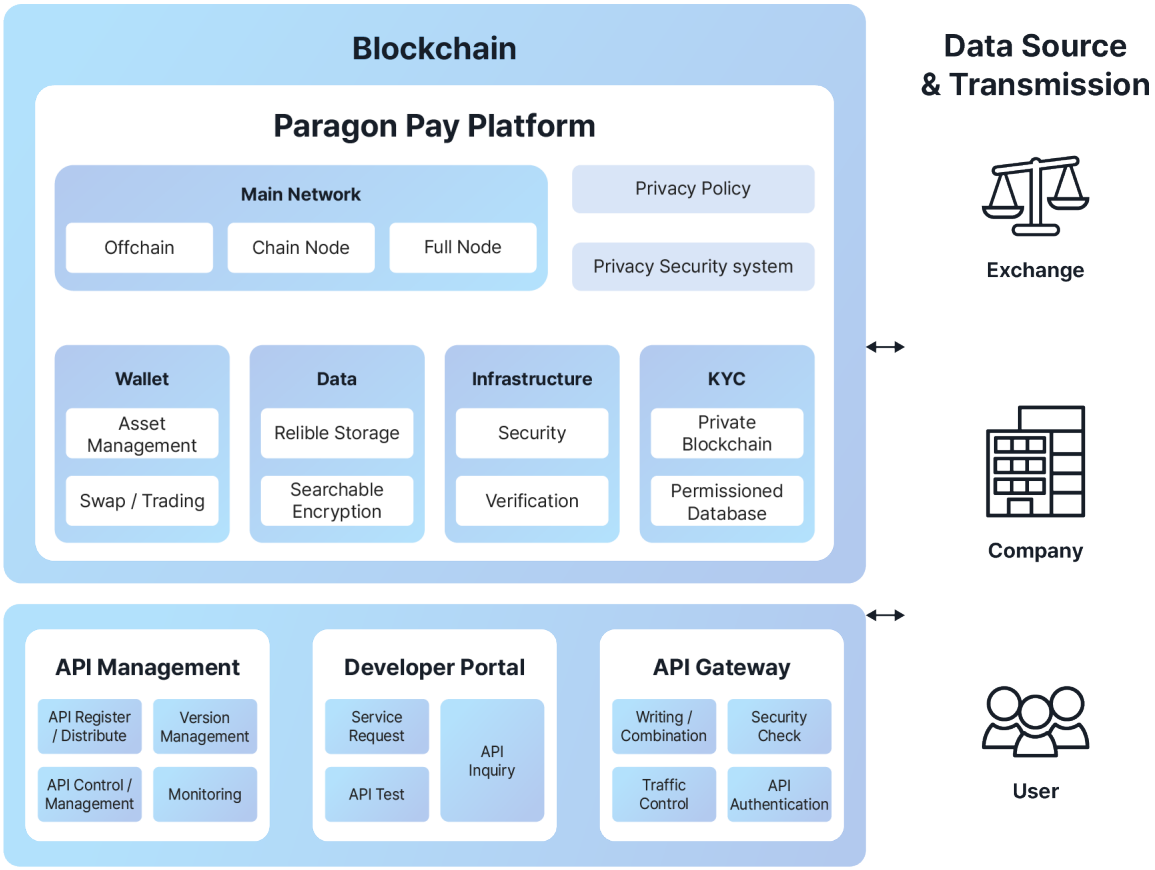
또한 ERC-20 표준을 지원하는 서비스 및 소프트웨어와 자동으로 호환됨을 통해 확장성을 지니게 됩니다. 이더리움 블록체인 자체가 하나의 플랫폼이면서 플랫폼 상에 구현되는 많은 솔루션들이 중앙 통제가 아닌 블록체인 기반의 탈중앙화가 핵심이면서 이를 통해 만들어지는 Dapp (Decentralized Application) 내에서 토큰 교환은 물론 다른 이더리움 상의 Dapp의 토큰과 교환이 가능해지도록 설계되었습니다. 이를 통해 익명성, 무국적성, 탈중앙화, 분산화 등 블록체인의 특성을 지니며 국가에서 직접적으로 통제하는 것이 불가능하고, Smart Contract를 통하여 각 사물 그리고 수많은 주체들과 계약을 통해 자동화된 경제 활동이 가능하다. 호환성과 관리가 쉬운 ERC-20을 통해 Dapp들 간의 상호작용을 증진시키고, 다른 토큰 간의 통합 시 오류와 버그 가능성이 줄어듭니다.

블록체인 기반 Smart Contract는 기본적으로 모든 트랜잭션 로그가 저장된 블록체인 데이터 베이스와 Smart Contract의 상태를 저장하는 데이터베이스 두 가지가 존재하는데, 이를 변경하기 위한 입력 값은 트랜잭션에 포함되어있습니다. 트랜잭션을 통한 인터페이스는 트랜잭션 데이터 베이스에 저장되고, Smart Contract의 상태를 변경시키는 방식으로, 모든 데이터를 공유함으로써 특정한 사용자가 Smart Contract의 실행 결과를 조작이 불가능하다는 특징을 가지고 있습니다. 블록체인이 모든 트랜잭션의 무결성을 보장해주는 방식으로 Smart Contract의 무결성을 보장할 수 있으며, 조건이 충족된 경우 자동으로 계약을 이행하여 계약의 집행 비용 및 분쟁 가능성을 줄입니다. Smart Contract 또한 웹 서버, 모바일, 일반 PC 어플리케이션 등 기존 시스템과 인터페이스를 통하여 계약 내용의 등록, 집행, 결과 조회 등의 동작을 수행할 수 있습니다. Paragon Pay의 Smart Contract 또한 오랜 기간 동안 비즈니스의 관행으로 고착화된 여러 단점들을 개선하고, 혁신을 통하여 새로운 가치를 창출하는 것을 목표로, 해킹 위험이 낮고, 보안 비용이 절감되며, 중개자가 없어 수수료 절감 및 데이터 정합성, 무결성 검증 시간이 단축되도록 개발되었습니다. 또한 계약의 투명성으로 인해 규제 비용이 절감되고, 이중 지불의 위험도 사라지며 정보 시스템 구축 비용이 절감되는 등 추가적인 메리트를 노릴 수 있습니다. 상호 약속된 규칙에 의해 절차로 작동되며 서로 간의 신뢰가 필요한 해당 서비스 같은 영역에서 가장 큰 시너지 효과를 보일 것으로 예측됩니다.

일정한 형식의 반복적인 계약이 많아지고, 원격자 간 계약 체결이 필요하며, 유통 추적이 필요한 Paragon Pay 플랫폼의 특성에 맞도록 개발되어 최적화된 생태계 환경을 제공하고자 합니다. Smart Contract에 기반한 DApp은 EVM을 통하여 임의의 복잡한 알고리즘 코드를 실행할 수 있는데, 네트워크에 참여하는 모든 노드는 블록 검증 프로토콜의 일부로 EVM을 실행하고, 네트워크 내 모든 노드가 실행함으로써 EVM을 통해 Smart Contract에 연관된 모든 트랜잭션을 실행하며 모든 노드가 동일한 계산을 수행하며 같은 값을 저장하는 구조입니다.

또한 대부분의 거래소와 지갑에서 인식 가능하며, 광범위한 교환에 적용할 수 있는 보편적인 프로젝트이자 대체 가능한 트레이딩 어플리케이션에도 탁월하고, 모든 거래가 승인되어야 하기에 총공급량이 유통 중인 토큰의 복사본이 없도록 하여 검증 프로세스를 원활하게 만든다는 특징이 있습니다. 다양하게 흩어진 ERC20 표준 호환 토큰들을 한 번에 ETH로 바꾸어 활용할 수 있습니다. ERC-20을 준수하기 위한 Contract에 필수 요소 및 부가적인 기능을 설정을 통해 유연성을 가짐으로써, Paragon Pay 플랫폼 개발에 적합한 부가적인 기능과 변수를 개발하여 관련 사업에 최적화된 플랫폼 구축을 목표로 두고 있습니다.

Architecture



Platform Structure

Paragon Pay는 기존의 서비스들보다 강화된 안정성과 기술력, 보안성을 바탕으로, 생태계에 참여하고 있는 사용자들에게 필요한 정보 및 결과값들을 제공하기 위하여 각 기술 레이어 간의 유동적인 처리 과정을 진행하며, 이를 통해 플랫폼 생태계를 확장해 나가는 것을 목표로 합니다. Paragon Pay는 블록체인이 갖는 투명성 및 보안 안정성, 기존 서비스의 성능과 확장성을 유지하기 위하여 다음과 같은 레이어로 구성됩니다.

Wallet

Paragon Pay 생태계에서 본인 소유의 계정을 접근하기 위한 Private Key를 제공하고, Wallet 모듈을 통하여 플랫폼 생태계 내의 경제 활동에 참여하기 위하여 필수적인 Key 정보를 안전하게 관리할 수 있도록 합니다. 이를 기반으로 Paragon Pay 생태계 내에서 진행되는 Contract에 관련한 안정성을 제공하고 폐쇄적인 동작을 보장함으로써 Key 정보 유출을 방지하고 안전하게 활용 가능한 보안 기능을 제공합니다.

Data

Paragon Pay 생태계에서 본인 소유의 계정을 접근하기 위한 Private Key를 제공하고, Wallet 모듈을 통하여 플랫폼 생태계 내의 경제 활동에 참여하기 위하여 필수적인 Key 정보를 안전하게 관리할 수 있도록 합니다. 이를 기반으로 Paragon Pay 생태계 내에서 진행되는 Contract에 관련한 안정성을 제공하고 폐쇄적인 동작을 보장함으로써 Key 정보 유출을 방지하고 안전하게 활용 가능한 보안 기능을 제공합니다.

Wallet

블록체인 플랫폼의 큰 특징인 신뢰 가능한 저장 공간과 객관적으로 탐색 가능한 암호화 기능을 제공합니다. 각 데이터는 블록으로 생성되어 탈중앙화 분산 원장으로 관리가 되며, 이를 통해 임의적인 조작이 불가능한 객관적이고 안전하고 공정한 블록체인 플랫폼 생태계를 제공합니다

Infrastructure

Paragon Pay이 실물 사업 및 다양한 프로젝트에 연계하기 위하여 구축된 레이어로써, 해당 레이어에서는 보안과 인증 기능을 제공합니다. 해당 레이어를 통하여 Paragon Pay는 다른 생태계의 쇼핑몰, 페이먼트, 블록체인 프로젝트 등과 연계를 통해 Paragon Pay의 생태계뿐만 아니라 다양한 생태계와의 연동을 통하여 플랫폼을 확장해 나갈 수 있습니다.

KYC

실물경제와 밀접한 Paragon Pay의 플랫폼 특성상, 본인 인증 및 신원 인증을 거쳐 안전하고 신뢰할 수 있는 플랫폼을 제공합니다. 플랫폼에 제공된 개인 정보는 블록체인을 통하여 안전하게 보관, 관리가 되며, 기존 신원 인증 방식들과 달리 금융 기관들의 관리 운영 비용에 비교하여서도 더욱 저렴하면서, 강화된 신원 정보 관리가 가능합니다. 이를 통해 플랫폼 내 거래에 있어 투명성을 높이고 거래 모니터링의 가시성을 높일 수 있는 특징을 지닙니다.

API Management

Paragon Pay의 사용자들의 생태계 참여 시 진입 포인트로써, 참여자들이 생태계 서비스에 직관적이고 안전하게 접근할 수 있는 기능을 제공합니다. 서비스에 대한 접근성을 제공하고 쉽고 편리하게 다양한 정보를 교환할 수 있는 특징을 지닙니다. 해당 레이어를 통하여 손쉽게 블록체인에 접근하고 서비스 레이어가 제공하는 다양한 서비스에 접근이 가능합니다. Paragon Pay는 꾸준한 관리 및 연구 개발을 통하여 더욱 발전된 플랫폼 생태계를 제공하는 것을 목표로 합니다.

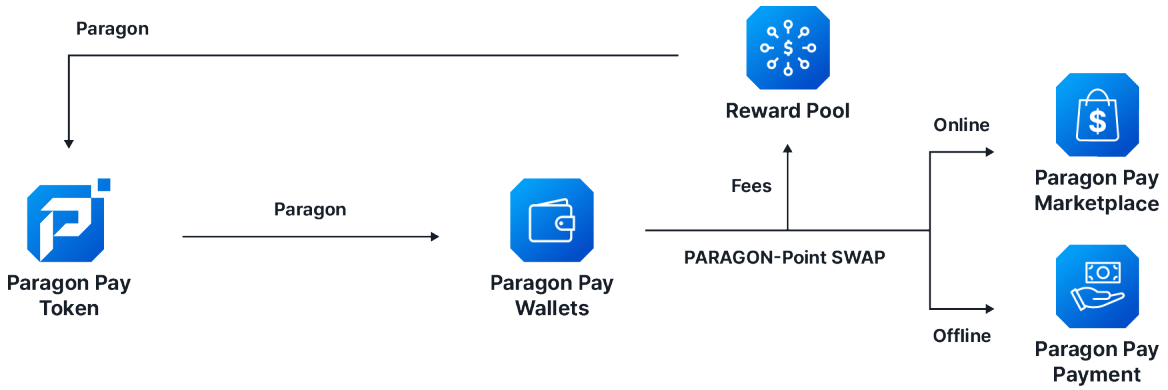
Developer portal

플랫폼 내부에서 진행하는 영역으로, 데이터 생성, 저장, 변경 방식을 결정하는 실제 프로세스 영역으로, 생태계 내 트랜잭션 정보를 다양하게 공유하고 단위 테스트를 위해 UI 외부에서 로직을 구축하였습니다. 플랫폼 내에서 다양하게 처리되는 영역을 최적화시켜 더욱 원활하고 쾌적한 사용 환경을 제공합니다.

API Gateway

플랫폼과 연계된 API 인증, 올바른 Backend로 API 요청 라우팅, 시스템 과부하 방지를 위한 Rate Limit 적용, 오류 및 예외 처리를 위한 다양한 기능을 제공하는 레이어로, 실시간 API와의 연동을 최적화합니다. 이는 Paragon Pay의 플랫폼과 연계된 API 트래픽을 빠르게 처리하고 리얼타임 아키텍처를 위한 가장 중요한 구성 요소를 담당하는 역할을 제공하는 레이어입니다.

04 Ecosystem



Paragon Pay Wallet

KYC를 진행한 유저들에게는 개개인의 블록체인 지갑이 생성됩니다. 이는 자신이 보유하고 있는 PARAGON 토큰을 포함한 다양한 가상 화폐의 수량을 확인 가능하고, 실시간 거래소 API와의 연동을 통하여 해당 가치 만큼의 PARAGON으로 교환이 가능합니다. 사용자는 Paragon Pay의 Marketplace 활용을 위하여, Wallet에 보유한 PARAGON을 포인트로 전환하여 사용이 가능하며, 포인트는 전환 시점의 PARAGON이 상장된 거래소의 시세에 적용되어 스왑 됩니다.

Reward Pool

Paragon Pay의 Reward Pool은 생태계 참여자들에 대한 다양한 보상 체계를 구축함으로써, 참여자들에게 다양한 혜택을 제공합니다. 리워드 풀에 예치된 PARAGON을 생태계 참여자들에게 보상으로 제공하는 선순환 구조로, 플랫폼 생태계 확장과 구축을 목표로 합니다.

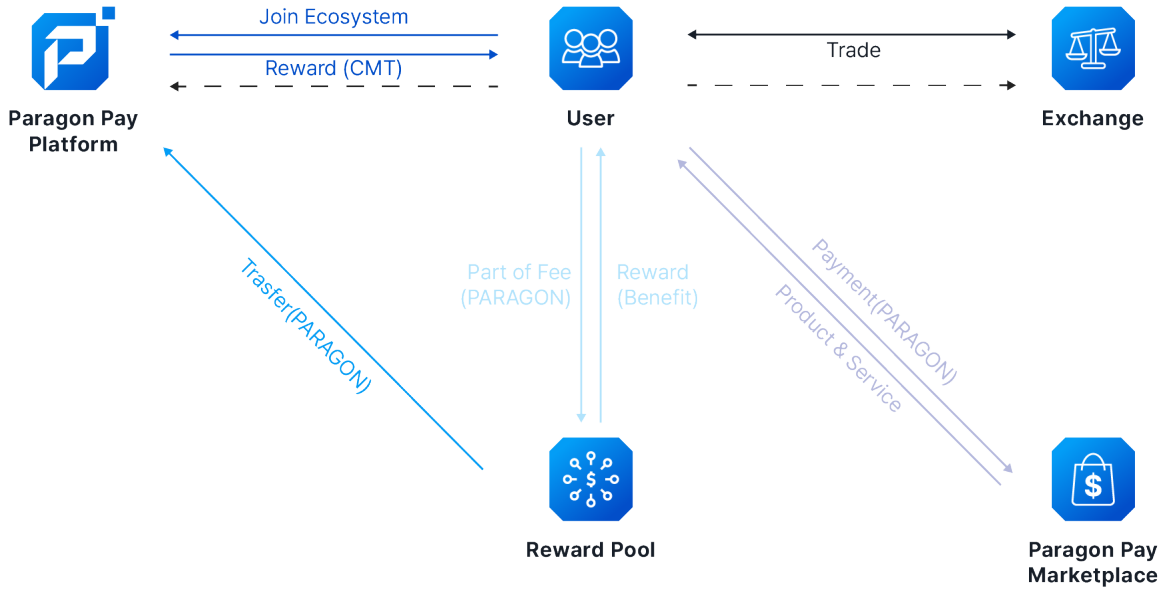
Payment

실물 기반의 플랫폼인 Paragon Pay는 보유하고 있는 PARAGON을 활용하여 실제 오프라인 매장 및 플랫폼 내 Marketplace에서 활용이 가능합니다. 생태계 참여자들은 Paragon Pay와 연계된 파트너 및 협업 프로젝트 등의 물품 및 서비스를 구매, 이용하는데 PARAGON를 활용하여 더욱 합리적이고 안전한 결재 시스템을 활용할 수 있습니다.

Marketplace

향후 사업 진행 방향에 따라, Paragon Pay 플랫폼 내 마켓 플레이스가 제공됩니다. 여기서 생태계 참여자는 보유하고 있는 PARAGON를 사용하여 Paragon Pay의 자체적인 제품이나 서비스, 또는 협력 및 파트너사의 제품과 서비스를 이용하거나, 기프티콘을 구매하는데 활용할 수 있습니다. PARAGON로 구매 시 일정 부분의 수수료가 발생하며, 이 중에서 일부는 리워드 풀로 이전하여 생태계 참여 보상으로 제공되는 선순환 구조를 제공합니다.

05 Token Economy



Paragon Pay에 기축 토큰으로 활용되는 PARAGON은 생태계를 지원하는 유틸리티 토큰으로, 개인 및 기업, 개발자 및 생태계 참여자들에게 블록체인 기술 및 암호화폐 관련된 모든 것을 지원하도록 설계되었습니다.

토큰 구매: Paragon Pay 플랫폼에서 제공되는 서비스를 사용하기 위하여 사용자들은 Paragon Pay 플랫폼 자체에서 직접적인 구매나, Paragon Pay이 상장된 거래소를 통해서 코인을 구매할 수 있습니다.

생태계 참여: Paragon Pay 생태계에 참여한 사용자들은 Paragon Pay 플랫폼에서 제공되는 서비스 활용, Marketplace 거래, 이벤트 참여 등을 통하여 생태계에 참여할 수 있으며, 이를 통해 생태계 기여에 따른 보상이 지급됩니다.

토큰 활용: 생태계 참여자는 보유하고 있는 PARAGON을 통하여 Paragon Pay 어플리케이션 내 제공되는 Marketplace에서 실물 상품이나 서비스, 기프티콘을 구매가 가능하며, Paragon Pay와 연계된 오프라인 매장 및 가맹점등에서 PARAGON 토큰을 활용할 수 있습니다.

암호 화폐 거래소 활용: Paragon Pay을 보유 중인 생태계 참여자들은 상장되어 있는 거래소를 활용하여 추가적인 투자 운용 관리를 할 수 있습니다. 이를 통해 부가적인 수익 창출을 기대할 수 있고, 여기서 확보된 수익을 통하여 다시 Paragon Pay 생태계에 참여할 수 있습니다.

06 Token Information

Paragon Pay 토큰 유통량 계획

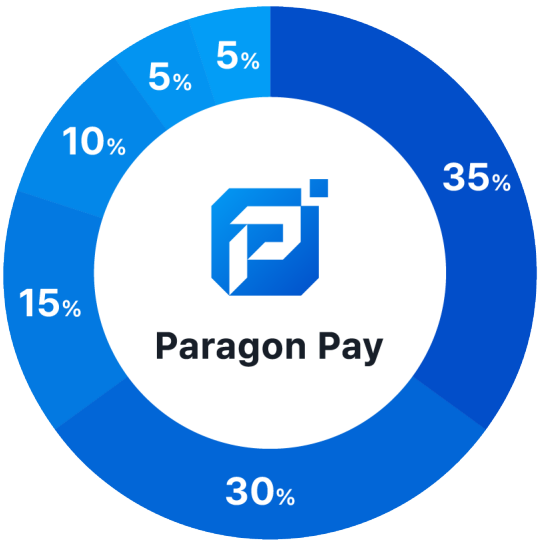
[1] Paragon Pay 정보

Paragon Pay 플랫폼 내 기축통화로 활용되는 PARAGON은 Ethereum 블록체인 네트워크 내 ERC20 규격 토큰으로 발행됩니다. PARAGON의 발행은 Paragon Pay 생태계에서 활용될 수 있는 어플리케이션 내 투자 및 정보 활용 등에 대한 개발과 거래, 생태계 참여를 위한 목적으로 발행되며 정보의 투명한 기록과 관리를 위한 생태계 조성을 위해 진행됩니다. 또한 다른 사업체와의 제휴, 협력 등 Paragon Pay 생태계의 확대를 위한 마케팅, 상장과 독자적인 블록체인 네트워크 개발, 유지보수, 플랫폼 구축, 시장 상황 변동에 대한 대비책 등에 활용될 예정입니다.

토큰 명칭	토큰 타입	총 발행량	소수점
Paragon Pay (PARAGON)	ERC-20	500,000,000 PARAGON	18

Token Address: 0xfe65601137c67537789Ce33fa0D49Df10F974F5E

[2] Token Allocation



- **Token Sale (35%)** 175,000,000 PARAGON
- **Ecosystem (30%)** 150,000,000 PARAGON
- **Marketing (15%)** 75,000,000 PARAGON
- **Foundation (10%)** 50,000,000 PARAGON
- **Development (5%)** 25,000,000 PARAGON
- **Advisor (5%)** 25,000,000 PARAGON

07 Road Map

2023

2Q

>> Paragon Pay 프로젝트 컨셉 수립

3Q

>> Paragon Pay Ecosystem 수립
>> Paragon Pay 정책 연구

4Q

>> Paragon Pay 플랫폼 개발 기획
>> PARAGON 토큰 개발 시작

2024

1Q

>> Paragon Pay 플랫폼 테스트 진행 및 런칭
>> 글로벌 시장 진출 기획
>> 글로벌 거래소 상장 진행

2Q

>> Paragon Pay 파트너십 확장

- 해당 로드맵은 사업 진행 방향 및 개발 진행에서 발생할 수 있는 변수에 따라 변동될 수 있습니다 -

08 면책조항

본 백서는 Paragon Pay 프로젝트가 추진하고자 하는 블록체인 기반 마일리지 포인트 관련 플랫폼의 새로운 사업 모델과 현황, 팀에 대한 정보를 제공하고자 작성되었습니다. 귀하는 본 문서와 문서에 명시된 정보에 접근함에 있어 다음 사항들에 대하여 동의한다는 것을 Paragon Pay에 무조건적이며 비가역적으로 진술 및 보증합니다.

1. 규제 국가에서 문서 접근 불가

특정 관할권에 있는 개인 또는 특정 범위에 속한 개인이 해당 문서를 보는 것은 합법적이지 않을 수 있습니다. 해당 백서를 보는 개인은 먼저 자신이 본 문서를 보는 것을 금지하거나 제한하는 법률 또는 규정에 해당되는지 확인이 필요합니다. 특히, 관련 법률과 규정에서 허가하지 않는 한, 본 문서에 언급된 코인 또는 토큰의 판매에 참여하는 것이 금지된 국가에서는 제공해서는 안되며, 문서를 직간접적으로 전송해서는 안됩니다. Paragon Pay는 본 문서에 대한 접근을 금지하는 법률이나 규정이 있는 지역과 문서의 일부가 불법일 수 있는 지역에서는 본 백서에 대하여 접근하는 개인에 대하여 책임지지 않습니다. 이에 따른 리스크는 스스로가 감수해야 합니다.

2. 정보 목적

Paragon Pay나 Paragon Pay의 직원, 임원 또는 어드바이저는 모든 정보에 대하여 어떠한 종류의 보증을 하지 않으며, 명시적이고 묵시적인 모든 보증과 조건을 부인합니다. Paragon Pay는 이러한 정보 및 정보에 있는 오류, 누락으로 인한 결과와 그로 인하여 발생된 결과에 대하여 귀하 또는 제 3자에게 어떠한 의무나 책임을 지지 않습니다.

Paragon Pay와 관련하여 해당 백서에 포함된 정보는 '미래 전망 진술'로 간주되는 언급이 포함될 수 있으나, 이는 역사적 사실에 근거한 진술이 아닙니다. 이러한 미래 전망 진술 중 일보는 '목적으로 한다', '목표로 한다', '예상한다', '믿는다', '할 수 있다', '추정한다', ' 기대한다', '만약,' '의도한다', '할 수도 있다', '계획한다', '가능하다' '있을 것 같다', '예상한다', '해야 한다', '할 것으로 보인다', '할 것이다' 또는 이와 유사한 용어와 같은 미래 전망 단어를 활용할 수 있습니다. 이러한 용어는 이 밖에도 더 있을 수 있습니다. 미래 전망 진술에는 미래의 사건이나 상황과 관련된 위험과 불확실성이 내재되어 있습니다. 따라서, 관련 기관에 대한 예상 로드맵, 개발, 예상 조건, 성과에 대한 본 문서의 추정과 예측치를 포함한 의견 및 미래 전망 진술에 대한 정보는 선별적이며 업데이트, 확장, 개정, 독립적인 검증 및 수정될 수 있습니다.

Paragon Pay는 본 백서에 명시된 정보의 진실성, 정확도, 완전성과 관련하여 어떠한 진술이나 보증, 약속을 하지 않습니다.

또한 Paragon Pay는 법에서 요구되는 범위 외에는 미래 전망 진술을 업데이트하거나 수정할 의무나 약속에 대하여 명백하게 책임을 부인하며, Paragon Pay나 관계자들의 미래 전망 진술에 언급된 모든 상황이 실제로 발생한다고 장담하거나 진술, 보증하지 않습니다. Paragon Pay는 본 백서에 명시된 모든 목표치를 달성하기 위하여 노력할 예정이나, 예상치 못한 변수나 상황으로 인하여 목표에 대한 변경이 가능하며, 별도의 통지 없이 해당 목표에 대한 달성을 하지 못할 수 있습니다.

3. 제안 없음

본 백서는 정보 제공 목적으로만 작성되었으며, 어떠한 형태의 투자, 증권, 기타 금융 상품에 대하여 구매, 판매, 청약, 인수를 제안하거나 형성하지 않습니다. 또한 본 문서의 어떠한 부분에서도 어떠한 방식으로든 이와 관련된 계약이나 투자 결정을 내리도록 제안하지 않으며, 이러한 결정의 근거로 사용되거나 의존할 수 없습니다.

4. 통지 없음

본 백서의 어떠한 내용도 법률, 금융, 세금, 기타 통지에 해당하지 않습니다. 귀하는 자체적으로 실사를 수행하여야 하며, 귀하의 관할지 내 디지털 자산, 세금, 증권, 기타 규정에 대한 모든 현지 법률을 준수해야 합니다. 관련된 전문가와 개별적으로 상담해 보시기 바랍니다.

5. 규제 위험

많은 관할지에서 디지털 화폐, 디지털 자산, 블록체인 어플리케이션을 포함한 디지털 토큰의 규제 상황은 명확하지 않거나 불안정합니다. 본 문서의 발행과 배포가 관련된 법률과 규정, 규칙을 준수했음을 의미하지는 않습니다. 그 어떠한 규제 기관도 본 문서를 검토하거나 승인하지 않았습니다. 관련 정부 기관에서 기존 법률, 규정, 규칙을 변경하는 경우 금융 기관에서 특정 상업적 결정을 내리는 경우, 본 백서에 언급된 모든 관련 사항들이 의도한 대로 기능 또는 작동할 능력에 중대한 악영향을 주거나 그러한 능력을 손상시킬 수 있습니다. 또한 본 백서를 어떠한 계약이나 투자 결정의 기초로 사용되어서는 안 됩니다.

6. 기타 면책 공고

이 문서는 Paragon Pay에 대한 정보를 담고 있으나, Paragon Pay 전체 내용을 나타내는 것은 아닙니다. 본 백서의 내용은 경영진의 판단뿐만 아니라 관련 법률 및 규정, 사업 상황, 업계 전망의 변화에 따라 변경될 수 있습니다. 정치, 사회, 경제, 주식, 디지털 자산 시장 상황 변화가 발생할 수 있으며, 관련 블록체인 시스템과 토큰을 수용 및 채택하는 일이 거의, 또는 전혀 없어서 관련된 블록체인 시스템과 토큰이 더 이상 상업적으로 사용이 불가능해질 수 있습니다. 제 3자의 웹사이트나 정보 출처에 대한 참조가 이루어졌을 경우, 당사는 해당 출처에 참조된 정보의 정확성, 완전성, 적시성에 대한 추가 검증을 요구하지 않았을 수 있으며, 이와 관련된 어떠한 보증도 하지 않습니다.