
PROT

CONTENTS

0. VISION

VISION

비트코인은 2008년 개발된 이후로 블록체인의 기술개발이 되었고, 수많은 개발자 등이 블록체인 개발에 참여하고 있습니다. 분산 플랫폼으로 블록체인 이더리움과 비트코인, 라이트코인 등이 있으며 이들은 디지털통화 개발에 중점을 두고 있습니다.

하지만 블록체인 기술이 급속도로 발전함에도, 앞으로 해결해 나가야 할 기술과제가 많이 발생하고 있습니다.

저희 Pine Platform 은 이 같은 문제점과 과제를 개선하기 위해 노력하고 있습니다. 암호화폐에 관련된 기술 및 개발 연구를 통하여 암호화폐 시장의 변화를 선도하고 혁신에 기여하고자 합니다

PROT 마스터노드 플랫폼은 개인 참여자들의 리스크는 최소화 시키고, 주기적인 마스터노드 보상을 안겨 줄 것이며, 시장에는 신뢰성, 접근성 및 적은 변동성을 제공해 줄 것입니다.

PROT는 궁극적으로 마스터노드 분야의 최초 기축 통화를 목표로 하고 있습니다.

PROT

I. INTRODUCTION

PROT

I. INTRODUCTION

1.1 PROT 소개

블록체인은 2009년 초 최초의 블록체인 가상 화폐인 비트코인의 시작으로 널리 보급 되었습니다. '나카모토 사토시'라는 비트코인 개발자가 새로운 탈중앙화 전자지불 시스템을 만들겠다는 구상으로 제기한 이 시스템은 '신뢰성이 아닌 암호학을 기초하여 합의에 이르는 제 3자가 없이 직접 지불을 진행할 수 있도록 설계 하였습니다.

그 때부터 비트코인을 비롯한 블록체인 기술은 전 세계적으로 널리 알려지게 되며 비트코인의 성공에 뒤이어, 다양한 블록체인 기술이 탑재 된 플랫폼들이 등장하였고 많은 알트코인들이 생겨났습니다.

과거에도 중앙집권적 실체는 사회적 구조가 진보하고 인류가 진보함에 따라 몰락하는 경우가 있었습니다. 인류의 진화에 미래를 결정하는 선택된 소수에 권력을 맡기는 것은 블록체인 P2P(Peer-to-Peer) 네트워킹이 만들어진 명확한 이유입니다.

현재 블록체인의 미래는 기술의 장점을 활용하고자 하는 정부기관, 금융기관, 글로벌 기업 등의 Needs가 확대 되면서 관련 기술 개발 및 활용에 적극성을 보이고 있으며 참여 또한 더욱 가속화 될 전망입니다.

이를 바탕으로 저희 PROT은 블록체인과 관련된 기술 및 개발 연구를 통하여 암호화폐 시장의 변화를 선도하고 혁신에 기여하고자 합니다

INTRODUCTION

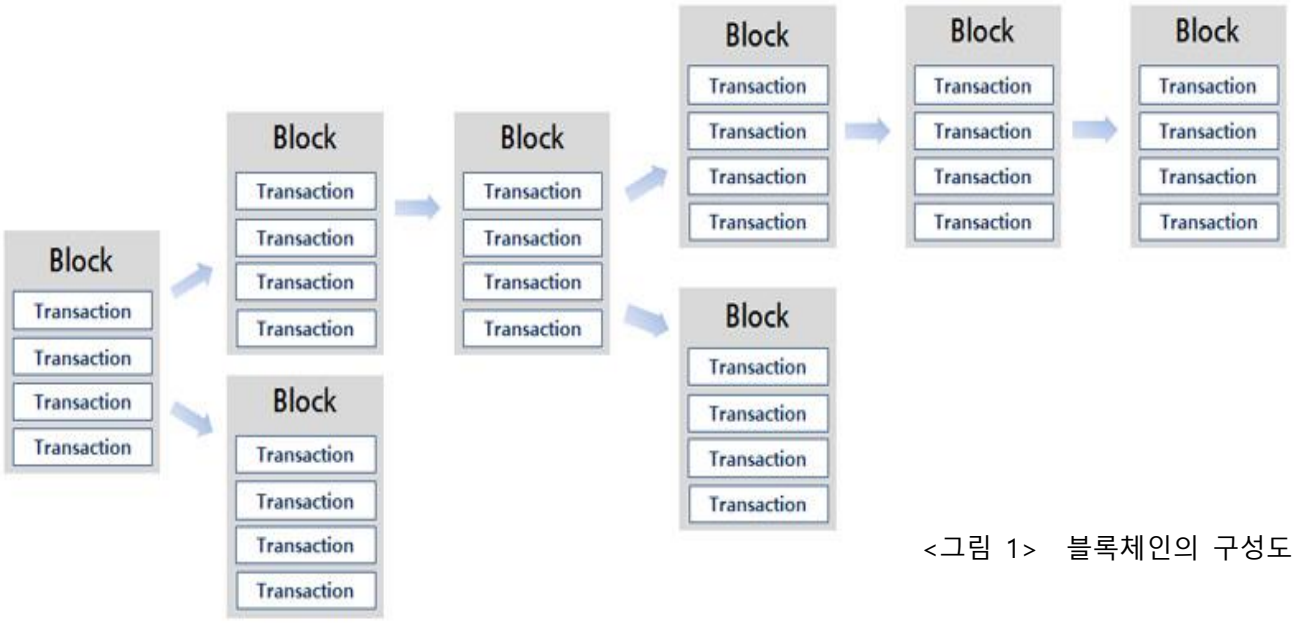
1.2 블록체인과 마스터 노드

블록체인은 데이터 분산저장 기술과 안전한 거래를 가능하게 하는 암호화 기술 그리고 분산된 정보의 정합성 유지 및 안정적인 운영을 위한 P2P(Peer to Peer) 통신 기술이 융합된 기술입니다.

기존의 데이터 베이스는 중앙에서 특정 조직이 데이터 베이스의 소유권을 가지고 사용자 간의 중간 중계역할을 하며 모든 데이터를 저장,검증 했습니다. 이러한 목적의 데이터베이스가 사용자,조직 사이에서 공유되는 경우는 매우 드뭅니다. 기술적 문제와 보안상의 문제가 있기 때문입니다.

가장 문제가 되는 것은 보안상의 문제입니다. 데이터베이스는 항상 위,변조의 위험에 노출되어 있고 데이터베이스를 관리하는 주체인 특정 조직은 위,변조의 위험에서 다양한 방법으로 데이터베이스의 보안을 지키며 저장된 데이터가 유효한 데이터임을 검증하고 여러 단계의 검증 로직을 개발,운용 합니다. 이는 관리의 비용을 높이며 데이터 베이스의 신뢰성을 보장하기 어렵게 합니다.

블록체인은 이러한 문제를 해결하고자 하는 방법중에 한가지 입니다. 안전성, 투명성과 더불어 효율성을 높이기 위해 설계되어졌으며, 각 사용자간 공유되는 거래의 비중앙집권적, 분산형 데이터베이스입니다.



<그림 1> 블록체인의 구성도

INTRODUCTION

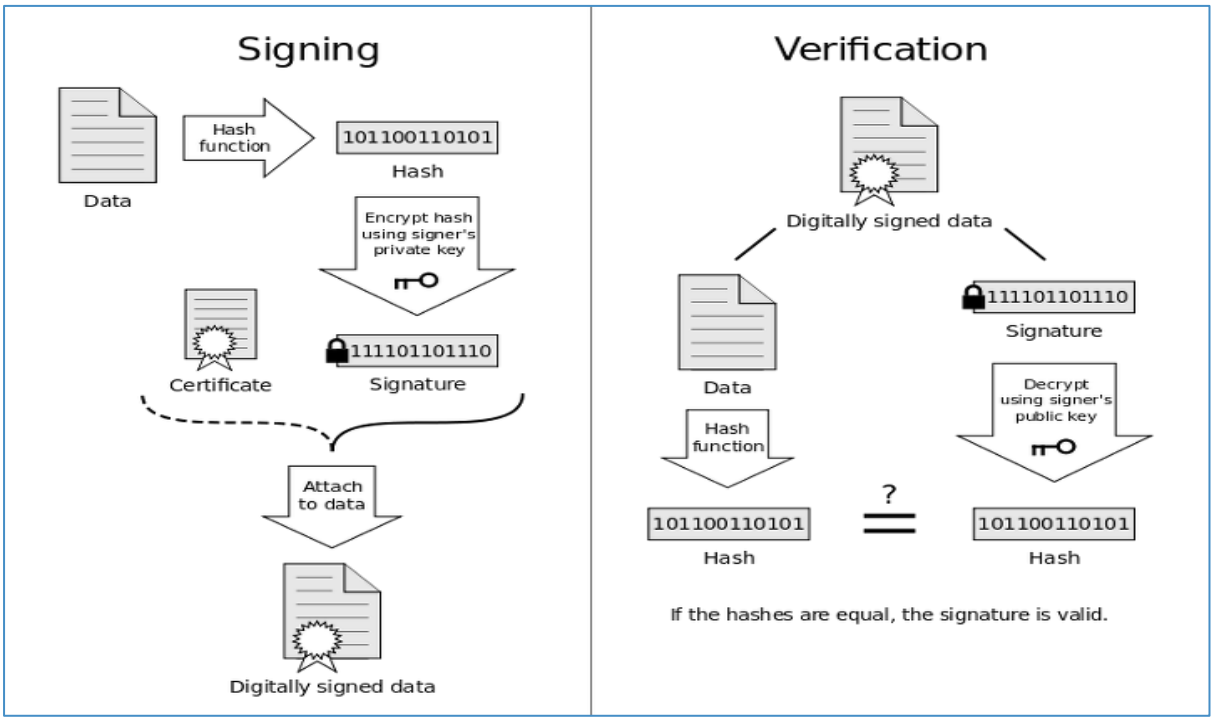
. 블록체인이 라는 것은 인코딩 결과가 모든 노드에서 동일하고 이전 트랜젝션 체인에 추가 된 공통 트랜젝션을 결합하여 암호화를 통해 전체 네트워크에서 유효성을 검사하는 블록으로 분할 된 트랜젝션의 데이터베이스 입니다. 블록이 무효화된 경우 노드의 '합의'에 의해 부적합 노드의 결과가 수정됩니다.

블록체인의 형태에는 누구나 거래 당사자로 참여할 수 있는 퍼블릭 블록체인(Permissionless)과 권한이 있는 사람과 기업만이 거래 당사자로 참여할 수 있는 프라이빗 블록체인(Permissioned)으로 나눌 수 있습니다.

퍼블릭 블록체인은 현재 암호화폐 시스템을 대부분이 채택하는 방식으로 암호화폐만 구매하면 누구나 퍼블릭 블록체인에 거래 당사자로 참여할 수 있으며 퍼블릭 블록체인은 신용있는 거래 당사자와 대규모 인프라 없이도 거래가 가능함을 보여주는 사례가 되었습니다.

프라이빗 블록체인은 권한 있는 거래 당사자만으로 블록체인을 구축해 블록체인의 단점이었던 느린 데이터 동기화 속도를 개선한 기술로 권한 있는 거래 당사자란 개인보다는 블록체인용 인프라를 제공할 수 있는 기업이나 관공서를 의미합니다. 참여한 당사자들이 적고 블록체인용 인프라의 질이 뛰어나기 때문에 거의 실시 가능한 상태로 전체 거래장부를 동기화할 수 있다는 장점이 있고 누구나 참여할 수 있고, 인프라 없이도 시스템이 유지된다는 당초의 목표는 조금 퇴색되었지만, 거래 장부의 위·변조가 불가능하다는 장점은 변함이 없습니다.

블록체인을 사용했을 때 기존 데이터 베이스와 차별화 되는 장점중 가장 중요한 것은 안정성,투명성,효율성으로 블록체인은 거래에 관하여 당사자의 신원을 확인하여 그 거래를 검증하기 위 한 암호화를 실시하고 있습니다. 이로 인해 당사자의 동의없이 블록체인에 가짜 거래를 추가 할 수 없습니다. 해시로 불려지는 복잡한 수학적 계산이 거래가 블록체인에 추가 될 때마다 실행되며, 그 블록체인은 거래데이터, 거래에 관련된 당사자의 신원 그리고 이전 거래의 결과와 이어져 있습니다. 블록체인의 현재상태가 이전의 거래에 의존한다는 사실은 악의를 가진 사람이 과거의 거래를 변경할 수 없는 것을 보장합니다. 이는 이전의 거래데이터가 변경되었을 경우, 현재의 해시값에 영향을 미칠 것이며, 거래원장의 다른 복사본과 일치하지 않기 때문입니다. 이는 안정성을 높이며 데이터 신뢰성을 높일 수 있습니다.



<그림 2> 블록체인의 진위여부 검증 도식

. 또한 블록체인은 여러 노드에 의해 유지관리, 동기화되는 분산 데이터 베이스 입니다. 또한 거래 데이터는 당사자간에 일관성이 있어야 하며, 이것이 첫번째 블록체인에 추가되어야 합니다.

이것은 설계 상 여러 당사자가 같은 데이터에 접근할 수 있다는 의미로 투명성이 높은 기술입니다.

효율적인 측면에서는 일반적으로 블록체인을 사용하여 복수의 데이터베이스 복사본을 유지하는 것이 단일 중앙집권적 데이터베이스보다 효율적이지 않다고 생각할 수 있느나 실제 대부분의 사례에서는 여러 당사자가 이미 동일한 거래에 관한 정보를 포함하는 여러 종류의 데이터베이스를 가지고 있습니다.

대부분의 경우 같은 거래에 관하여 데이터 가 동일하지 않아 조직 간에 시간과 비용을 들여 조정하는 절차를 필요로 합니다.

조직간에 블록체인 등의 분산 데이터베이스시스템을 사용하면, 사람 손에 의한 조정의 필요성이 경감되어 상당한 비용이 절감됩니다.

또한 블록체인은 조직간 중복 작업의 필요성을 없애 공통 및 상호기능을 개발 할 수 있는 기회를 제공합니다.

INTRODUCTION

. 코인을 채굴하는 방법은 크게 작업증명 방식(Proof of Work)과 지분증명 방식(Proof of Stake)이 있습니다.

Proof of Work (이하 POW) 방식은 해쉬 파워가 높을수록,코인을 얻을 수 있는 블록을 더 많이 발견할 수 있는 시스템으로 블록이 생성되는 시간을 일정하게 유지하기 위해 '난이도'라는 개념이 존재해 총 해쉬량이 증가함에 따라 채굴 난이도가 상승하게 되고, 상승된 난이도에 따라 블록을 찾는데 더 많은 해쉬가 요구되기에 블록 자체가 생성되는 시간은 일정하게 유지되는 시스템 입니다.

하지만 이런 POW 방식은 높은 전력의 소모, 비싼 채굴장비(ASIC, GPU등)의 구비와 해쉬 독점으로 인한 보안문제와 중앙화 이슈 등이 있습니다. 현존하는 대부분의 코인들은 POW 방식을 채택하고 있으며, 대표적으로 비트코인, 라이트코인, 이더리움 등이 있습니다.

Proof of Stake (이하 POW) 방식은 POW 방식의 가장 큰 단점인 채굴 및 유지에 들어가는 과도한 비용(장비구입, 전기료 등)과 해쉬 독점으로 인한 보안 이슈를 해결하고자 고안된 방식으로서, 전체 코인에 대한 자신의 참여율에 따라 추가적으로 발행되는 코인에 대한 획득량도 달라지는 방식입니다.

즉, POW 방식에서 '해쉬'의 역할을 POS 방식에서는 '지분'이 하게 되는 것 입니다. 또한 POS 방식은 코인을 보관하고 있는 각각의 지갑을 연동시켜 놓는 것만으로도 강한 보안 장벽을 만들어 낼 수 있는 장점이 있습니다.

최근에는 POS 방식을 기반으로 한 코인들이 많아지는 추세이며, 기존 코인들도 POW 방식에서 POS 방식으로의 변화를 꾀하고 있습니다. 대표적인 예로는 이더리움이 있습니다.

POW (Proof of Work)	
코인의 분배	- 해쉬값 (HASH) 의 크기
장점	- 현재 주류 코인들이 사용 - 높은 시장 가치 형성
단점	- 높은 전력소모 - 지속적으로 해쉬 (HASH) 의 유지가 필요 - ASIC (전용채굴기) 및 GPU (그래픽카드) 구매비용 필요 - 낮은 Transaction Fee (수수료)

POS (Proof of Stake)	
코인의 분배	- 보유한 코인의 지분 (Stake)
장점	- 채굴에 들어가는 비용 유지 비용 최소화 (PC 1대 + Internet 연결이 전부) - 네트워크의 분산화로 안정성 확보 Pump and Dump 의 최소화
단점	- 낮은 네임 벨류 (Name Value) - POS노드에 대한 정보가 부족하여, 일반인들이 접근 하기에 어려움

<그림 3> POW / POS 비교

INTRODUCTION

Proof of Stake + Master Node

Master Node 란?

› " Master Node(이하 마스터노드) 란 쉽게 설명하자면 은행의 예금의 형식과 비슷하다고 볼 수 있습니다. "
› 마스터노드는 POS (지분증명방식) 즉, 일정 지분의 코인을 가지고 해당 코인을 "채굴"하는 방식입니다.
› 마스터노드를 운영하기 위해서는 해당 코인의 담보가 필요하며 그 담보를 대상으로 서버를 이용 가능하게 하며 그에 대한 댓가로 주인에게 보상을 제공하는 방식입니다.

Master Node (이하 마스터노드)는 암호화폐 네트워크에 존재하는 노드로서 거래를 중개해주는 것 외에도 다른 특별한 기능을 하는 노드를 지칭합니다.
마스터노드의 가장 두드러진 특징은 특정 마스터노드를 운영하는 사용자가 일정 기간 이후 해당 노드에서 생성된 보상을 자신이 참여한 암호화폐의 형태로 받을 수 있다는 점이며, 이 때 보상은 블록체인상에 존재하는 해당 코인의 총 마스터노드 개수와 운영 기간에 따라 상이 할 수 있습니다.

참여자들은 원하는 마스터노드에 일정량 이상의 코인을 락업해 둠으로써 별도의 채굴이나 거래 없이도 주기적으로 마스터노드 운영 보상을 받을 수 있으며, 마스터노드에 참여하기 위해서는 직접 서버를 구축하거나 서비스 제공자의 도움을 빌려 마스터노드를 구성해야 합니다.
이는 에너지 절약의 측면에서 매우 효율적이며 투자적 관점에서도 기존 암호화폐와 다른 새로운 기회를 제공하지만 앞서 서술한 바와 같이 직접 서버를 구축해야 한다는 점은 진입장벽을 높이며 소수의 전문가들만 참여하는 문제가 있습니다.

마스터노드는 POS 채굴 방식을 지향합니다. 채굴은 난이도에 따라 블록 생성 주기가 변하게 되며, 블록체인상에 구성 된 마스터노드의 개수에 따라 보상이 변하게 됩니다.

II . BACKGROUND

PROT

II . BACKGROUND

PINE PLATFORM은 핀테크 회사를 설립하였고, PINE PLATFORM은 PROT Coin 암호화폐 연구소를 개설하여 4차 산업의 다양한 기술들을 개발하고 있습니다.

핀테크(Fintech)는 금융(Finance)과 기술(Technology)을 결합한 용어로 글로벌 IT 기업이 폭넓은 사용자 기 반을 바탕으로 송금, 결제, 대출, 자산관리 등 각종 금융서비스를 결합하여 제공하는 새로운 유형의 금융 서비스를 말합니다.

핀테크의 등장은 스마트폰 이용의 보편화로 소비자의 소비행태가 모바일 중심으로 변화하고 있고, 빅데이터 분석 등으로 소비자에게 맞춤형 금융서비스가 가능해진 것을 의미 합니다.

핀테크는 전자상거래와 금융서비스가 새롭게 만나면서 자연스럽게 생겨난 현상으로 PROT Coin 컨소시엄 핀테크는 랜딩, 빅데이터, 플랫폼, 크라우드 펀딩, 간편 결제 및 송금 서비스 등 다양하고 실용적인 핀테크 금융서비스를 제공하며 핀테크 허브 플랫폼을 목표로 PROT 플랫폼을 개발 하고 있습니다.

PROT Coin 핀테크의 네 가지 큰 특징으로는 간편성, 보안성, 경제성, 신속성을 꼽을 수 있으며 이는 핀테크 허브 플랫폼으로 써의 역할을 수행하기 위해 중요한 요소 입니다.

네 가지 특징의 목표와 개념은 다음과 같습니다.

› **간편성** : 기존의 암호화폐들은 컴퓨터 엔지니어 커뮤니티 중심으로 개발되어 대중적인 접근은 다소 간과 되었습니다.

지불의 증명은 직관적이지 않았고 어플리케이션의 메소드들은 엔지니어들만 사용할 수 있었습니다.

또한 기존의 대중적인 지불수단과는 다른 사용자 경험을 제공했고 블록의 싱크를 동기화하는 과정은 엔지니어에게 조차 명확성을 제공하지 못했습니다.

PROT의 간편성은 암호화폐를 통한 지불, 송금, 보증등이 대중적인 마그네틱 기반 카드 결재보다 쉽게 대중적으로 사용되기 위함입니다.

코어와 통신하는 메소드는 랩핑(Wrapping)되어 json 형태로 제공될 것이며 빠른 처리속도와 연동된 동기화 통신을 지원할 것입니다.

BACKGROUND

› **보안성** : PROT의 보안성은 누적 신뢰 점수를 기반으로 하는 무작위 분산 데이터 클러스터링을 통해 진일보한 보안성을 보장할 것이며 각각의 노드는 다른 노드의 신뢰 점수와 응답속도를 고려해 서로 통신하며 검증합니다.이는 51% 공격과 같은 블록체인에 대한 악의적 공격과 전통적인 소셜 해킹 시도에 대해 보다 나은 보안성을 보장할 것 입니다.

› **경제성** : 블록체인의 근간인 분산원장 기술에서 관리 비용을 제외한 전체 데이터 저장 비용의 총합은 불가피하게 중앙 집권적 시스템보다 커질 수 밖에 없습니다. 참여하는 노드들에게 분산되어 중앙 관리비용이 필요하지 않지만 근시일 내에 개인이 감당하기 어려운 비용에 도달할 것은 자명합니다. 일반 적으로 블록당 2MB의 저장공간을 필요로 하고 생성 주기가 1분 이하인 현재의 상황으로는 대부분의 프로젝트들이 상정하는 기간인 30년 이내에 32테라바이트가 필요합니다.

32테라 바이트에 달하는 데이터를 읽고 쓰는데 현재와 같은 환경이 보장될 가능성은 없습니다. PROT는 이에 대한 대안으로 근본부터 다르게 설계된 분산원장 시스템을 제안합니다.

각각의 노드들에게 과거의 기여와 활동을 토대로 신뢰 점수가 매겨질 것이며 신뢰 점수와 각 노드의 자원 상태를 고려한 클러스터링으로 네트워크 비용은 보다 더 분산될 것입니다.

이로 인해 PROT는 모바일 기기 같은 자원이 낮고 민감한 디바이스에 포팅되어 핀테크 허브 플랫폼의 기반을 구축할 것입니다.

› **신속성** : 경쟁에 기반한 채굴에서 벗어나 지분 증명과 신뢰도 기반 채굴 시스템으로 네트워크의 신뢰성을 공격하는 해킹과 유효하지 않은 블록의 생성을 막아 1블록 컨펌으로도 그 유효성을 보장하는 네트워크가 되면 블록생성 주기와 TPS 경쟁과 무관하게 빠른 트랜젝션 속도를 보장할 수 있게 됩니다.

이를 위해 PROT은 단편화된 네트워크와 노드 신뢰도 검증을 기반으로 설계되었습니다.

BACKGROUND

PROT의 철학

PROT Coin의 컨소시엄 핀테크 철학으로는 유저 중심의 서비스, 혁신적 아이디어와 기술, 명확한 정체성, 환경을 이해하는 구체화된 설계, 가치창출을 통한 인류 전체에게 돌아가는 서비스를 꼽을 수 있습니다.

프로젝트의 기술적 설계는 모두 공개될 것이며 설계 단계부터 사용자 중심의 서비를 위한 시스템으로 설계 되었습니다.

철학의 구현

블록체인기술은 초 연결(hyper-connectivity)과 초지능(super intelligence)으로 정의되는 제4차 산업혁명을 이끌 핵심기반 기술로 주목 받고 있는 가운데 제일 먼저 관심을 끌고 있는 것이 '가상화폐 코인'과 '코인 상장거래소' 이고 세계경제포럼 (World Economic Forum, WEF)에서는 2025년까지 전 세계 CDP의 10%가 블록체인 기반기술에서 발생할 것으로 전망 하고 있습니다.

블록체인(blockchain)기술의 분산된 데이터베이스 환경(Distributed Database Environment), DLT(Distributed Ledger 가상화폐거래소와 Technology), P2P 전자화폐 시스템, 분산 거래장부 (Distributed Ledgers) 등의 기술로 개발하여 거래소의 시스템 활용가치도가 높게 연동시키고 안전한 결제와 환금성을 높이기 위한 설계가 포함되어 있으며 PROT의 목표인 모바일 디바이스 포팅 단계에서는 블록체인 노드, 결재, 계약에 관한 데이터 외에도 노드가 된 디바이스의 방대한 데이터가 PROT 플랫폼의 활용성을 높이며 노드의 기여를 받음과 동시에 노드에게 무형, 유형의 자산과 기회를 제공할 것입니다.

이는 단순히 사용성 측면에서의 사용자 중심의 서비스가 아닌 사용자의 참여로 확장되는 구조로 진정한 의미의 전체를 위한 생태계라 할 수 있으며 그 결과물은 전체에게 공정히 공유되는 시스템 입니다.

III. PROT PROJECT

PROT

3.1 PROT의 구조

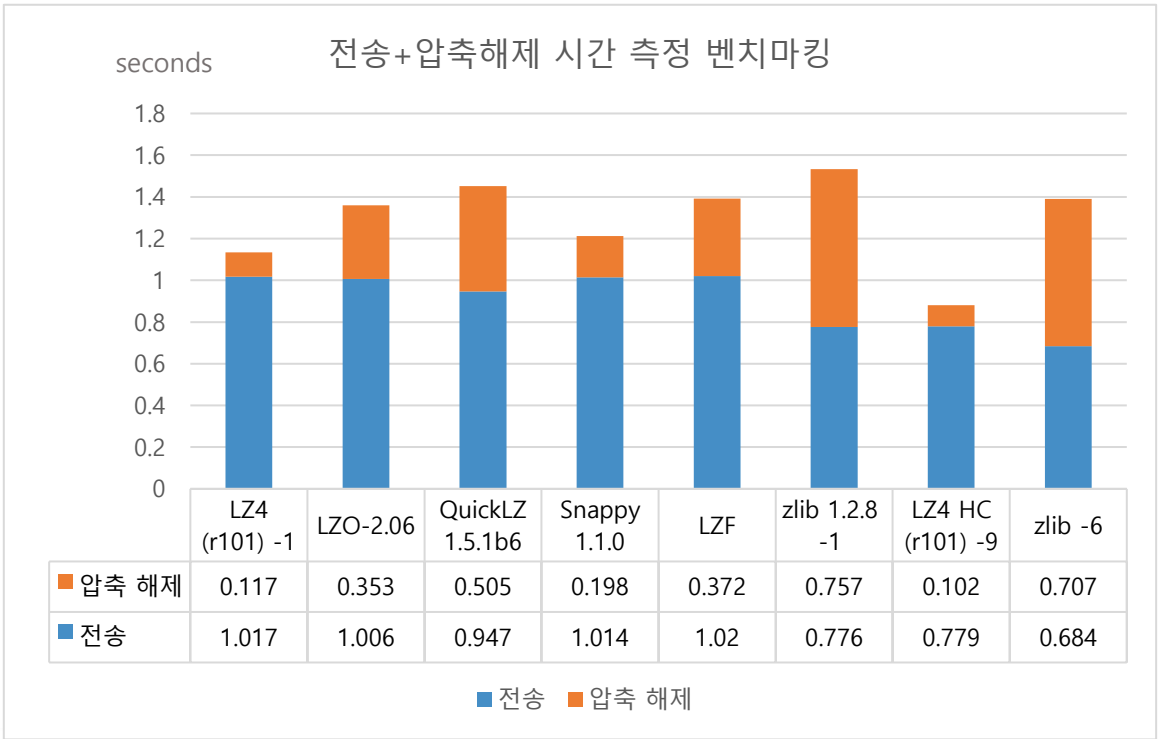
3.1.1 PROT의 기본설계

PROT는 DASH의 X11 마이닝 알고리즘을 기반으로 시작하여 기존의 기술은 포크하지 않은 새로운 클러스터링 마스터 노드를 목표로 하고 있습니다.

보상과 투표,거버넌스 설계는 동일한 구조를 계승할 것이며 일정은 로드맵에 공개될 것입니다.

우리가 전략적 클러스터링이라고 명명한 네트워크는 각자의 클러스터들이 동일한 원장을 보유하고 있지 않습니다. 30개의 클러스터는 역할에 따라 다시 3개의 큰 블록으로 나누어 집니다.

각 블록의 역할은 읽기전용, 전체블록데이터저장, 최신상태정보 저장으로 나누어 지며 각각의 역할, 상태에 따라 차이는 있지만 30GB 이내로 제한 될 것입니다. 읽기전용 블록은 오래된 트랜잭션의 데이터를 LZ4HC -9 알고리즘으로 압축되어 저장되고 APPEND, WRITE는 지원하지 않습니다.



	LZ4 (r101) -1	LZO-2.06	QuickLZ 1.5.1b6	Snappy 1.1.0	LZF	zlib 1.2.8 -1	LZ4 HC (r101) -9	zlib -6
압축 해제	0.117	0.353	0.505	0.198	0.372	0.757	0.102	0.707
전송	1.017	1.006	0.947	1.014	1.02	0.776	0.779	0.684

<그림 4> LZ4HC -9 알고리즘 벤치 측정값

PROT
PROJECT

READ ONLY 로 READ 메소드만 보유한 블록은 INCOMING 연결은 제한적으로 사용되며 외부와 합의 없이 자체적으로 129,600 블록 단위로 뒤쳐진 블록들을 저장합니다.

전체블록을 저장하는 블록은 고가용성 머신을 대상으로 하며 읽기전용 블록의 역할과 최신상태 정보 저장 블록의 역할을 동시에 하며 백업 노드로서 역할을 하게 됩니다.

기존 블록체인 노드와 동일하게 높은 자원소모를 담당하는 노드로 높은 신뢰도 점수와 높은 네트워크 가용성을 필요로 합니다.

최신상태정보 저장 블록은 259,200블록을 초과하여 뒤쳐진 블록을 1,440블록 주기마다 삭제하며 노드중 가장 비중이 높은 블록입니다.

네트워크의 가용성, 처리한 트랜잭션, 온타임 시간등을 고려해 신뢰도 점수가 매겨지며 높은 신뢰도 점수를 가진 노드의 데이터는 읽기전용 블록에서 참조하게 됩니다.

각블록은 다시 10개의 클러스터로 나눠지며 각 클러스터들은 물리적 지역,네트워크 가용상태,스토리지 가용상태를 서로 통신하며 하나의 블록으로서 유기적인 역할을 하게 됩니다.

3.1.2 x11 마이닝 알고리즘

X11은 DASH 코어 개발자인 Evan Duffield가 만든 널리 사용되는 해싱 알고리즘입니다.

X11의 연쇄 해싱 알고리즘은 작업 증명을 위해 11개의 과학적인 해싱 알고리즘을 사용합니다.

이것은 처리 분배가 공정하게 이루어지고 코인이 Bitcoin과 동일한 방식으로 배포될 수 있도록 하기 위한 것입니다. X11은 ASIC의 생성을 훨씬 더 어렵게 만들려고 했으므로 채굴 중앙 집중화가 위협이되기 전에 화폐 개발에 많은 시간을 할애했습니다.

이 접근 방식은 대체로 성공적이었습니다. 2016년 초 현재, X11 용 ASIC가 존재하며 네트워크 해시 속도의 상당 부분을 구성하지만, Bitcoin에서 나타나는 집중화 수준에는 이르지 않았습니다.

PROT
PROJECT

X11은 DASH에 (2014년 1월에 "Xcoin"으로 출시) 도입된 체인화 된 작업 증명 (PoW) 알고리즘의 이름입니다.
Quark의 연쇄 해싱 방식에 부분적으로 영감을 얻어 해시의 수를 늘림으로써 "깊이"와 복잡성을 추가했지만, Quark와 다른 점은 해시가 무작위로 추출되는 대신에 선험적으로 해시가 결정된다는 점입니다.

X11 알고리즘은 11개의 다른 해시(blake, bmw, groestl, jh, keccak, skein, luffa, cubehash, shavite, simd, echo)의 여러 라운드를 사용하므로 현대 암호화폐에서 사용되는 가장 안전하고 정교한 암호화 해시 중 하나입니다.

PROT의 프로토타입은 X11 알고리즘을 사용하여 개발 되었습니다.

3.1.3 Proof Of Work

초기 암호화폐는 중개자 없이 P2P 거래가 발생할수 있는 분산되고 불변한 원장을 유지하는 수단으로 사용 됩니다.
분권화되어 있기 때문에 비트코인은 운영 또는 유지 관리를 위해 어느 한 지점이나 기관에 의존하지 않고 오히려 네트워크 자체에서 발생하는 트랜잭션을 확인 하는 노드 네트워크에서 작동합니다. PROT도 이러한 비트코인의 기본 속성을 계승합니다다.

비트코인인은 원장의 무결성을 유지하기 위해 네트워크의 광산 컴퓨터의 처리 능력에 의존합니다.
트랜잭션은 각각 블록이라고 하는 데이터 청크로 기록됩니다. 따라서 블록 체인으로 조정 된 원장 (블록 체인)은 해싱 할 임의의숫자 (nonce)를 식별하여 암호화 컴퓨터의 처리 능력을 이용하여 암호 퍼즐을 해결합니다.

이러한 채광에 대한 의존도는 작업 증명 (Proof of Work, PoW) 시스템으로 알려져 있습니다. 네트워크가 성장함에 따라 이러한 암호 퍼즐이 어려워지고 해결하기가 쉽지않아 더 많은 처리 능력이 필요하게 됩니다.

PROT PROJECT

비트코인과 달리 PROT는 PoW에 의존하지 않습니다. Proof of Work 시스템의 중요한 문제는 블록 해시를 해결하고 증가하는 처리 요구 사항을 피하기 위해 경쟁 우위를 유지하지 못하도록 함께 작업하는 컴퓨터 그룹이 마이닝 풀에 대한 인센티브를 제공한다는 것입니다.

이 방법은 개인 채굴업자를 밀어 광산 풀의 처리 능력으로 이어지며 근본적으로 네트워크가 성장함에 따라 네트워크 속도를 저하시키고 많은 에너지를 소비하므로 환경에 부정적인 영향을 줍니다.

라이트코인은 암호화 알고리즘을 사용하여 비트코인보다 블록을 해시하는 것이 더 빠르지만, 채굴을 위한 채굴장비의 비용은 훨씬 제한적이라는 점에 유의해야 합니다. 256 및 Scrypt 기반 PoW 블록체인 모두 ASIC (Application-Specific Integrated Circuits) 채굴업자가 등장함에 따라 집중화의 가능성과 그것이 가져오는 위험이 더욱 분명 해졌습니다.

PROT
PROJECT

3.2 PROT 특징

3.2.1 PROT WALLET

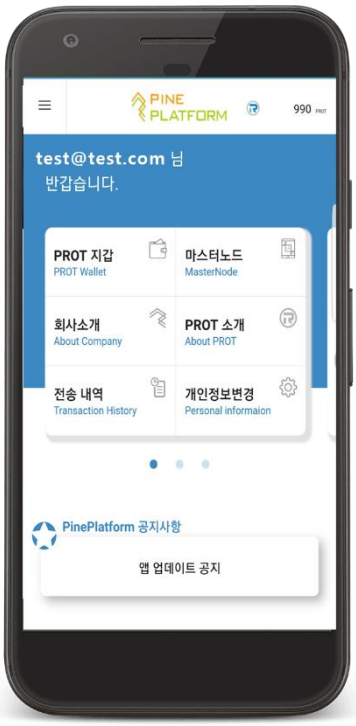
Pine Platform에서 제공되는 PROT Wallet은 암호화폐의 활용을 위해 제공되는 서비스 입니다. PROT Wallet은 Pine Platform에서 발행되는 PROT Coin을 안전하게 보관하며 RPC를 통해 노드와 통신합니다.

- 프라이빗 키 서버 보관

서버 보관에 대한 약관 동의 후 정책에 따라 프라이빗 키를 PROT Wallet 서버에 암호화하여 저장하며 분실시 개인 인증 후 프라이빗 키 복원이 가능합니다. 약간의 보안 위험성이 존재하지만 사용자 편의성을 위한 기능으로 선택적인 기능입니다. 악의적인 공격에 대비해 저장,이동이 2단계의 절차로 보안될 것이며 서명시 트랜잭션의 성격에 따라 서명이 제한되거나 추가 인증 절차를 수행합니다.

- 프라이빗 키 APP 보관

서버보관 지원과 동일한 단점이 존재하지만 이를 극복하기 위해 모바일 디바이스에 연동된 비가역적 암호화를 통해 디바이스 종속적 수단을 제공합니다. 이로써 모바일 어플리케이션에 저장하여 간편하게 사용 할 수 있도록 구성합니다. 프라이빗 키 분실의 우려가 적습니다..



<그림 5> PROT Wallet Main 화면

PROT
PROJECT

- 마스터노드 구축

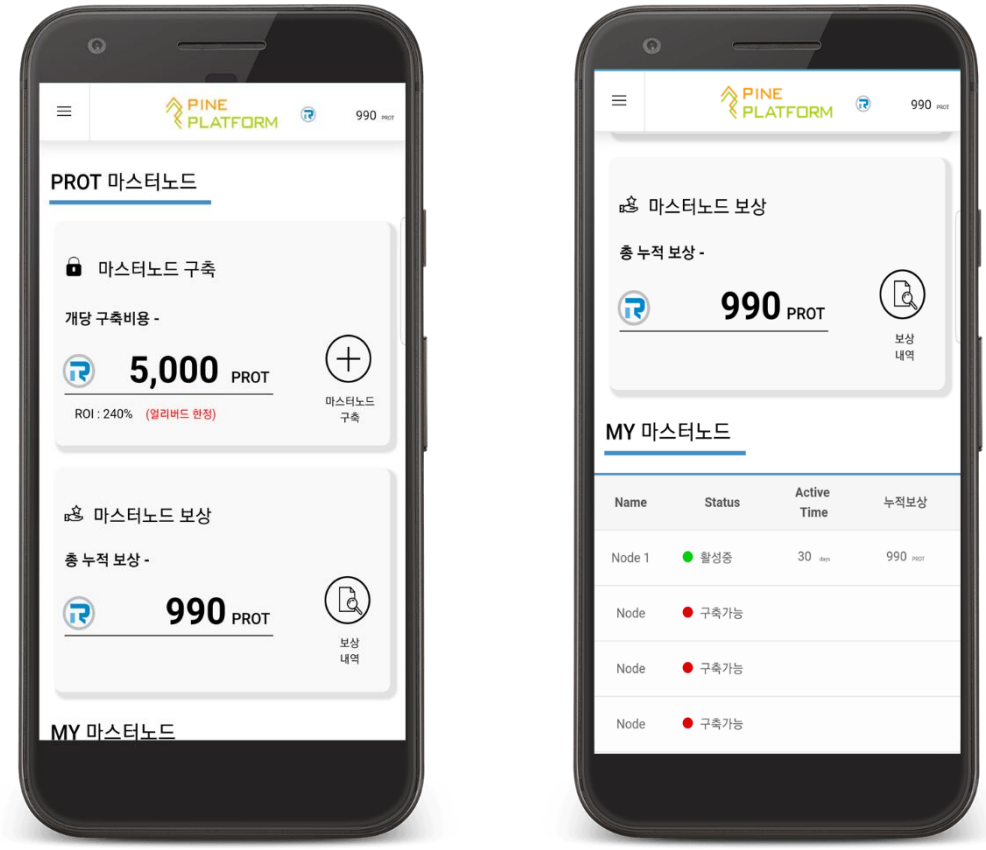
마스터 노드의 현황을 파악하기 위한 도구들을 좀더 편리하게 제공하기 위해 QT WALLET의 지원은 한정적일 것이며 모바일 어플리케이션 중심의 서비스를 제공합니다.

보유한 PROT Coin을 언제든지 마스터노드 서버를 구축할수 있으며, 수익률 차트를 제공함으로써 언제든지 수익 확인이 용이하며 상황에 따라 On/Off가 가능합니다.

내장된 블록 탐색기로 블록의 RAW DATA의 열람도 가능하며 PROT Wallet은 편리하고 안전한 서비스 제공을 목적으로 개발된 소프트웨어 Wallet입니다.

멀티 지갑 구조를 사용하여 다양한 방식의 암호화폐를 보관하고 사용 할 수 있으며, PROT Wallet을 통하여 지불결제 서비스의 사용이 가능합니다.

이러한 사용성과 안정성의 확보를 기반으로 사용자는 세계 어느 곳에서나 거래소와 연동하여 즉시 다른 화폐와 교환 가능합니다.



<그림 6> PROT Wallet 마스터노드 In App

PROT
PROJECT

3.2.2 PROT Wallet 주요 특성

..

- **보안성** : PROT Wallet은 사용자의 개인키(private key)가 생성되어 로컬 장치에 저장되며 외부 서버로 전송되지 않습니다. 사용자는 자신의 자산을 완벽하게 제어하고 보호할 수 있습니다.

- **익명성** : PROT Wallet은 사용자 자신을 식별하거나 정보 확인할 것을 요구하지 않습니다. 이 것은 사용자의 차별 및 개인 데이터 유출의 위험을 제거합니다.

- **편의성** : PROT Wallet은 사용자에게 익숙한 인터페이스로 PROT Coin의 송수신에 이용할 수 있으며, 입점한 제휴사를 통한 쇼핑몰결제, 마일리지/포인트의 전환에 이용할 수 있습니다.

- **다양성** : PROT Wallet PROT Coin 뿐만 아니라, 비트코인, 이더리움, 대시, 리플 등 다양한 코인을 안전하게 보관할 수 있습니다.
향후 더욱 다양한 코인을 지갑에 보관 하기 위해 계속적인 개발을 진행해 나갈 예정입니다. 또한 지갑 내에서 코인을 전환하는 기능을 추가하여, 코인을 전화하기 위해 지불되는 이중, 삼중의 수수료 문제도 해결할 계획입니다.

PROT
PROJECT

3.2.3 익명전송

PROT의 익명전송은 코인조인이 향상되고 확장된 형태입니다. 코인조인의 핵심적인 개념에 추가하여, 저희들은 분권화, 체인 접근법을 통한 강력한 익명성, 교단 및 수동적인 시단대 별 혼합과 같은 일련의 개선 사항들을 채택합니다.

암호화 화폐의 사적인 자유와 대체 가능성을 개선 할 때 가장 큰 과제는 블록 체인 전체를 모호하게하지 않도록 하는 것입니다.
비트코인 기반 암호화 통화에서는, 누구나 사용되지 않은 출력과 그렇지 않은 출력들 (일반적으로 UTXO로 알려진, UTXO는 사용되지 않은 거래 출력을 뜻함)을 구별할 수 있습니다.
이로 인해 어떠한 사용자든 거래의 무결성을 보증하는 역할 수 있는 공용 원장이 되는 상황으로 연결됩니다.

비트코인 계획안은 신뢰할 수 있는 거래 상대방이 부재시의 그들의 참여 없이 작동할 수 있도록 설계됐으며, 공용 블록체인을 통해 감사 기능들을 사용자가 쉽게 이용할 수 있는 것은 결정적입니다.

통화 내에서 분산된 혼합 서비스가 있음으로써, PROT는 통화 자체를 완벽하게 대체 가능하게 할 수 있는 능력을 얻습니다.
대체 가능성은 통화의 모든 단위가 평등하게 유지됨을 통재하는 속성입니다. 사용자가 통화 내의 돈을 수령하면, 이전 사용자들의 기록과 같이 오지 말아야합니다.
그렇지 않으면 사용자들은 그 기록에서 그들을 분리하여 모든 코인들을 동일하게 유지해야합니다. 동시에, 어느 사용자든 다른 사용자들의 사생활을 손상키지 않으면서 공공 장부의 재정적 무결성을 보장하기 위한 감사원을 역할을 수행할 수도 있습니다.
대체 가능성을 개선하고 공개 블록 체인의 무결성을 유지하기 위해, 저희는 사전에 분산된 신용 없는 혼합 전략을 사용하는 것을 제안합니다. 화폐를 대체성을 효과적으로 유지하기 위해서, 이 서비스는 통화에 직접 내장되어 있습니다.

PROT
PROJECT

3.3 Proof Of Stake

2 계층 네트워크인 PROT는 스테이킹 및 마스터노드 계층의 참여자에게 네트워크의 상태를 유지할 수 있도록 장려합니다.
POS를 통해 네트워크에 기여하는 사용자는 네트워크를 지원하기 위해 마스터노드에 대한 담보로 5,000 POT를 저장하여 보상을 받습니다.
이 두 가지 모두 시간의 경과에 따라 보상을 받는 수단이지만, 양과 수단은 다릅니다.

3.3.1 마스터노드와 스테이킹

PROT의 POS 스테이킹과 마스터노드 보상은 다른 마스터노드 기반의 암호화폐와 비슷한 매커니즘으로 동작합니다.
하지만 PROT는 선발 암호화폐들이 답습한 결과를 반영하여 비선형 함수의 보상 테이블을 제공합니다.
이는 각 구간별 마스터노드 참여자 들의 수와 그 참여자 들의 수익율을 이상적인 범위로 조절할 것입니다.
PROT의 마스터 플랜을 성공적으로 수행 하기 위해 마스터노드 공여자들의 역할은 크다고 할수 있습니다.

저희는 공여자 들의 프로젝트에 대한 기여에 매우 감사할 것이며 그에 따라 공여자들의 자산가치와 성공적인 수익을 위해 비선형적 보상 계획을 만들었고 스테이킹과 마스터노드의 균형 사이에 마스터노드에 좀더 높은 비중을 두었습니다.
마스터노드는 네트워크에 가장 중요한 기여를 하는 참여자임을 PROT는 충분히 이해하고 있으며 마스터노드에 안정적인 보상과 마스터노드 자산 가치의 보호가 최우선의 가치입니다.

PROT
PROJECT

3.3.2 마스터노드 참여

마스터노드로 작동하려면 5,000 POT를 사용할 수 없는 상태로 두어야 하며 24시간 인터넷에 연결되어있는 WINDOWS, LINUX 기반 컴퓨터가 필요하며 고정적인 IP주소가 필요합니다
상세한 설정법은 GITHUB와 공식 웹사이트를 통해 안내될 것입니다.

PROT는 현재 마스터노드의 구축의 과정이 대다수의 사람들에게 매우 번거롭고 어려운 작업임을 인정합니다.
또한 구축 후의 관리도 직관적이지 않으며 몇가지 오류들과 번거로운 절차, 그리고 어려운 콘솔 커맨드가 필요한점도 알고 있습니다.

이러한 문제들은 누구나 사용하기 편리한 플랫폼에 큰 장애가 될것이므로 PROT의 마스터 플랜에는 대단히 쉽고 편리하며 빠른 마스터노드 구축과 운영 툴이 포함되어 있습니다. 이는 휴대폰으로 알람을 맞추는 수준으로 간편한 작업이 될것입니다.

3.3.3 스테이킹 참여

PROT의 스테이킹은 사용자가 원하는대로 스테이킹을 선택하고 해제 가능하며 보유한 POT의 수량에 관계없이 수행할 수 있습니다.
보상의 균형은 기존의 마스터노드와 다소 다릅니다.

PROT는 마스터노드에 집중하고 있으며 소스의 하이 스테이커의 출현을 반기지 않습니다.
또한 스태이킹의 특성상 비전문가에게 진입 장벽이 높은 편이며 마스터노드의 가치를 희석할 가능성을 최소화 하고자 불균등 보상을 제시합니다.

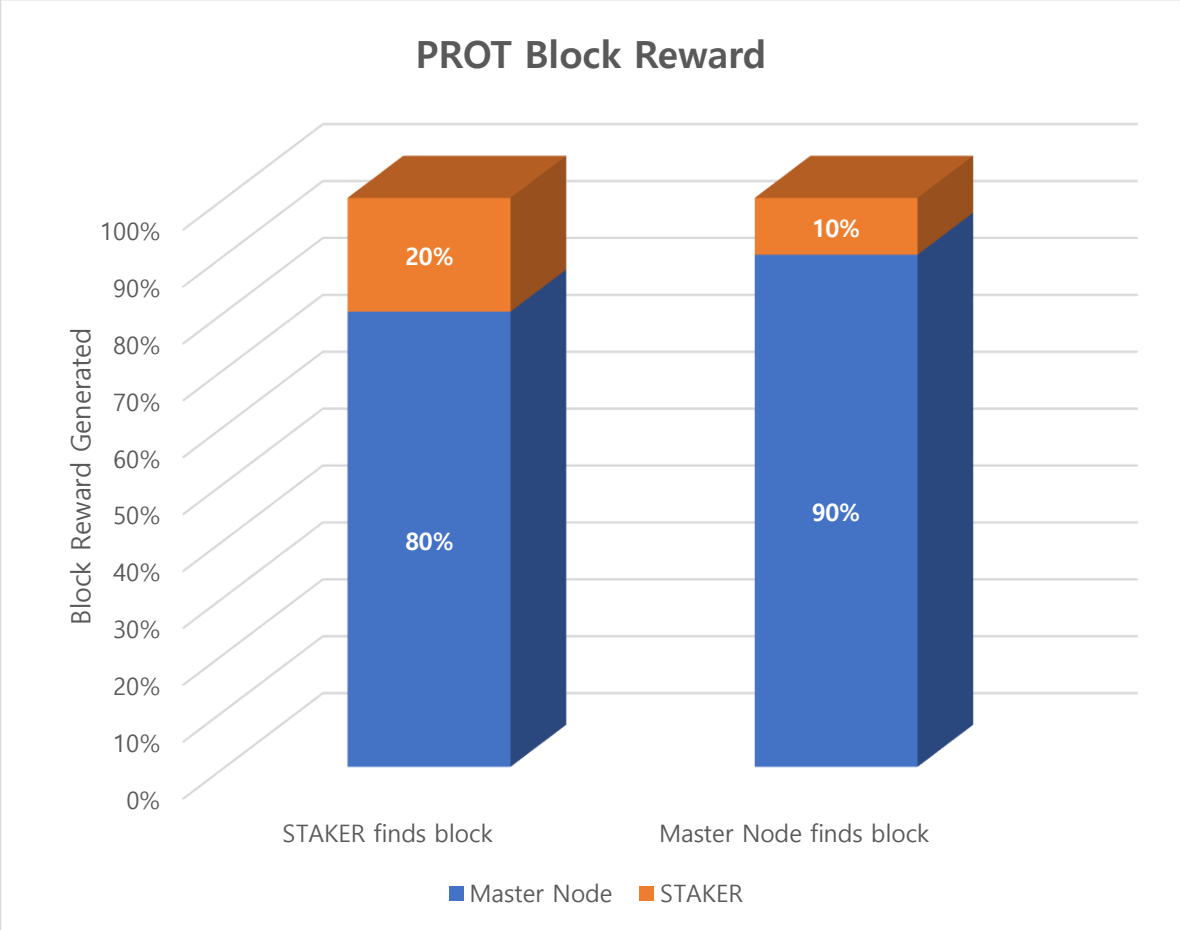
PROT PROJECT

3.3.4 보상 균형

기존의 마스터노드들은 스테이킹의 임의적인 체킹 특성으로 인해 동일한 양의 코인을 보유하는 마스터노드 보상보다 더 많은 보상을 얻을수 있는 가능성이 존재합니다.

한편 이는 평균적인 기대 금액보다 적은 보상을 받을수도 있는것을 의미 합니다. 이를 방지하고자 격차가 큰 불균등 보상을 제공하며 평균에 가까운 보상을 약속합니다.

PROT STAKER finds block: 마스터노드 80%, 스테이커 20%
Master Node finds block: 마스터노드 90%, 스테이커 10%



<그림 7> PROT 보상 MN · STAKE 보상 비율

3.3.5 PROT 보상 테이블

PHASE	BLOCK HEIGHT	TOTAL BLOCK REWARD	Master Node, POS REWARD	Governance RESERVE
1	100-43299	5	4.5	0.5
2	43300-86499	10	9	1
3	86500-129699	15	13.5	1.5
4	129700-172899	20	18	2
5	172900-216099	25	22.5	2.5
6	216100-259299	30	27	3
7	259300-345698	20	18	2
8	345699-432098	15	13.5	1.5
9	532099-518498	10	9	1
10	518499-1036887	8	7.2	0.8
11	1036888-16804888	6	5.4	0.6

<그림 7> PROT 보상 테이블

IV. BUSINESS MODEL

PROT

"4차 산업혁명이 시작되면서 블록체인과 함께 등장한 암호화폐는 탈중앙화, 익명성 그리고 신뢰성을 기반으로 다양한 분야에서 신규 참여자들의 이목을 끌고 있습니다. 그럼에도 불구하고 큰 가격변동성으로 인해 많은 사람들이 아직 암호화폐 를 "투기"로 보는 경향이 있으며, 이 때문에 사회적 문제가 될 것이라는 우려를 자아내고 있습니다.

PROT 마스터노드 플랫폼은 개인 참여자들의 리스크는 최소화 시키되, 주기적인 마스터노드 보상을 안겨 줄 것이며, 시장에는 신뢰성, 접근성 및 적은 변동성을 제공해 줄 것입니다. PROT 는 궁극적으로 마스터노드 분야의 최초 기축 통화를 목표로 하고 있습니다."

4.1. 마스터 노드 거래소

우리는 마스터노드의 보상이 예측에 가깝고 평균과 큰 차이 없이 배당 되도록 하고자 합니다. 하지만 현재 대다수의 마스터노드 암호화폐들은 보상과 수익 계산을 정확하게 하기 어렵습니다.

이를 보완하기 위해 블록생성 내역등의 블록 내역을 공개하는 경우도 있지만 일반적으로 널리 사용되기에는 어려움이 있으며 거래도 비트코인 계열과 이더리움 계열의 POW 채굴방식의 코인에 최적화된 기존의 거래소에서 이루어 지므로 마스터노드 코인의 정확한 가치와 비전, 검증, 거래에 적잡하지 않은 사실에 새로운 수요와 기회가 존재 합니다.

기존의 암호화폐 거래소가 존재하는데도 불구하고 왜 마스터노드 전용 거래소가 필요한지에 대해 의문을 가진 사람도 있을수 있으나 마스터노드 암호화폐는 기존 암호화폐와 구분되는 특성이 존재합니다.

그로인해 블록생성 내역, 분배의 확인,수익율의 현황, 전체 규모등 기존 암호화폐보다 참고할 정보들이 존재하며 기존 암호화폐와 달리 단순한 가치 저장의 수단으로써의 화폐가 아닌 그 자체로 투자의 수단이 되는 특수한 성질이 있습니다.

따라서 기존의 암호화폐 거래소에서는 이러한 마스터노드 암호화폐 거래를 온전히 지원하지 못하고 있습니다. 이러한 특성에 관한 정보에 이르는 과정은 간단하지 않습니다.

이를 보완하여 마스터 노드 전용 거래소 에서는 다음과 같은 주요 특성이 포함됩니다.

PROT
BUSINESS
MODEL

- 향상된 블록 탐색기

향상된 블록 탐색기에는 각 개발 주체별로 제공되는 데이터를 통합하여 일관된 인터페이스와 서로 일치하지 않은 공개범위에 따른 데이터 불균형을 해소합니다.
이러한 데이터가 통합이 되면 비교가 가능해지고 활용이 용이해 집니다.

기본적인 공급량, 현재블록 높이, 최근 보상내역, 최근 전송내역등의 데이터가 규격화된 프레임워크를 통해 서로 비교가 가능해지며 추가로 코인의 시간 흐름별 예측 공급 그래프, 과거의 공급 추세, 마스터노드의 분포와 전체 가용 컴퓨팅 파워 조회를 통해 각 코인의 미래와 가치를 가늠해 볼 수 있습니다.

- 기존 암호화폐와의 거래

국가별 제약을 줄이기 위해 모든 거래는 법정화폐가 아닌 비트코인과 이더리움을 거래 수단에 포함시킵니다.
이는 거래소의 국가적 제약을 줄이며 경제적으로 유리하며 직관적인 거래를 지원할 것입니다.

추가로 PROT는 비트코인,이더리움과 함께 거래소의 기축통화로 활용되며 인센티브 시스템을 통해 PROT 사용을 장려할 것입니다.

- 마스터노드,스테이킹 지원,대행

마스터노드 암호화폐은 앞서 서술한 그 자체로 투자의 수단이 되는 특성이 있으나 그 과정이 존재합니다.
단순히 지갑에 암호화폐를 보유한 것으로는 마스터노드가 될 수 없으며 스테이킹도 불가능합니다.
이는 현존하는 모든 마스터노드 암호화폐가 공통적으로 가지고 있는 문제이며 PROT는 이를 보완하는 최초의 마스터노드 암호화폐가 될 것 이지만 다른 코인들의 지원을 위해 직접 설치와 대행 설치를 모두 지원합니다.

PROT
BUSINESS
MODEL

직접 설치를 원하는 사용자를 위해 OS별로 빌드된 최신 코어를 거래소 내에서 제공할 것이며 국가별 언어로 번역된 상세한 매뉴얼이 포함됩니다.
또한 초기 블록 싱크 과정에서 발생하는 지연과 오류를 줄이기 위해 최신 블록 데이터 덤프를 제공합니다.
대행 설치를 원하는 사용자는 VPS 비용에 준하는 비용으로 거래소에 마스터노드 설치와 스테이킹을 일임할 수 있습니다.
이 경우에는 보안을 위해 추가적 인증을 진행할 것이며 중지는 일정 수준으로 제한될 것 입니다.

4.2 마스터 노드 연계 증권

마스터노드 암호화폐의 보상은 블록 주기별, 마스터노드의 적용수, 스테이킹정책 등의 요인으로 코인별 격차가 대단히 큽니다.
그러나 코인 개별적은 물론이며 평균을 적용해도 법정화폐나 기존의 암호화폐 대비 매력적인 수익률을 보여주고 있습니다.
하지만 아직 정보가 부족한 탓에 개인이 개별 코인을 선택하기 어려운 경우가 많으며 수익률의 변동이 큰 경우가 있어 이를 보안하는 마스터 노드 연계 증권을 거래소를 통해 공급할 예정입니다.
이해를 돕고자 연계 증권이라는 용어를 사용했으나 암호화폐를 자산으로 하는 기존 상품이 존재하지 않아 정확한 용어는 아닙니다.
주식시장에서 다수의 종목을 묶어 해당 종목 집단의 지수와 연계해 수익이 결정되는 연계증권처럼 엄선된 다수의 마스터 노드 상품을 한 자산으로 묶어 위험을 햇지하며 안정적인 수익을 추종하는 상품입니다.

PROT
BUSINESS
MODEL

4.3 PROT 모바일 플랫폼

PROT의 마스터 플랜이 완성되면 기존의 PC, VPS등을 이용하여 마스터노드를 적용하거나 스테이킹을 하는 불편함이 사라집니다.

모바일 어플리케이션에서 누구나 쉽게 마스터노드의 적용·해제 / 스테이킹의 적용·해제를 할 수 있으며 그 과정이나 결과 또한 매우 직관적이며 정확하게 이용자에게 전달될 것 입니다.

최소한의 모바일 디바이스 자원을 사용하도록 설계되었기 때문에 사용자는 일반적인 지갑 어플리케이션을 사용하는것과 큰 차이를 느끼지 못할 것이며 추가적 자원 사용은 30%이내로 제한될 것입니다.

모바일 플랫폼이 기존의 PC기반 노드를 모두 대체하고 클러스터링이 적용되면 마스터노드의 증가세가 더 상승할 것이며 PROT 플랫폼은 블록화된 클러스터링 네트워크를 통해 방대한 양의 데이터 가용 성능과 사용자 데이터를 활용할 수 있게 됩니다.

이를 바탕으로 PROT는 서브 코인을 동일 네트워크에서 발행 가능해져 지역 특수화폐 같은 추가 프로젝트를 포함하게 됩니다.

모바일 기반에서 축적된 빅데이터 자산과 물리적 지역과 연동되는 코인은 추가적인 시너지를 발생시켜 PROT 플랫폼의 영역을 확장할 것이며 기존 기업과 연계를 통해 플랫폼 내에서의 코인 발행을 협력,지원하여 PROT 모바일 플랫폼을 차세대 암호화폐 허브 플랫폼으로 발전 시킬 것 입니다.

V. ROAD MAP

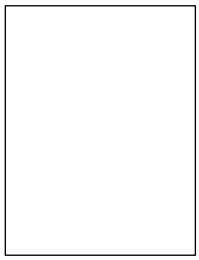
PROT

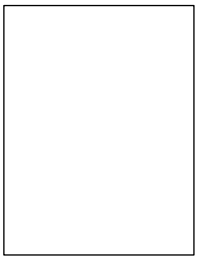
V . PROT ROAD MAP

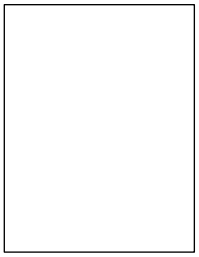
VI. TEAM MEMBER

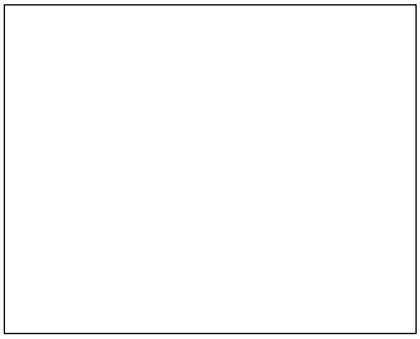
VII. TEAM MEMBER

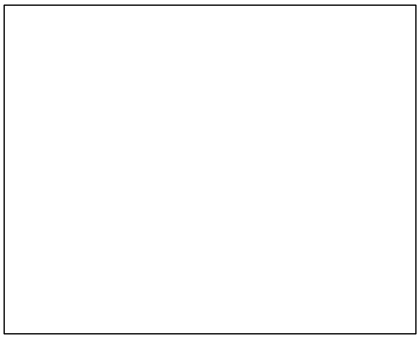
PROT TEAM MEMBER

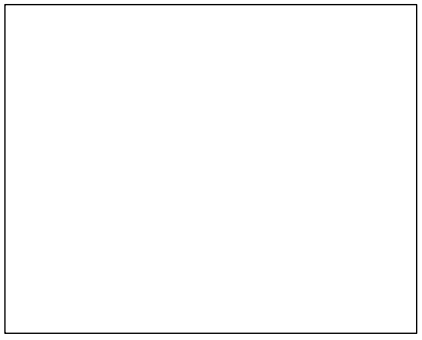












VII. REFERENCE

VII. REFERENCE

- Blockchain.info. (2012). Bitcoin Median Transaction Confirmation Time (With Fee Only). Retrieved 9/ 15, 2017 from https://blockchain.info/fr/charts/avg-confirmation-time

- DASH Masternodes - https://dashpay.atlassian.net/wiki/display/DOC/Masternode

- Bitcoin - https://bitcoin.org/bitcoin.pdf

- PIVX – https://pivx.org/wp-content/uploads/2019/05/PIVX-White-Paper-Sept-2018.pdf

- Crosby, M., Nachiappan, Pattanayak, P., Verma, S., et al., 2015. BlockChain technology

- Chang, S.-J., Perlner, R., Burr, W.E., Turan, M.S., et al., 2012. Third-round report of the SHA-3 cryptographic hash algorithm competition.

- Wiecko, R., 2017. Dash instamine issue clari cation.

- M.Vukoli'c The quest for scalable blockchain fabric: Proof-of-work vs. bft replication. International Workshop on Open Problems in Network Security,pages 112~125. Spriger, 2015

- "MasterNodes.Online." - https://masternodes.online/

- "Proof of Work vs Proof of Stake: Basic Mining Guide - Blockgeeks." https://blockgeeks.com/guides/proof-of-work-vs-proof-of-stake/

- LZ4 "lossless compression algorithm bench" - https://lz4.github.io/lz4

- AwadElkarim, FathElrahman. 2018. "On the scalability of blockchain"

REFERENCE

- 배봉진, 부산대학교 대학원. 2017 "Hash-based signature scheme for blockchain"

- Dinh, T. T.; Liu, R.; Zhang, M.; Chen, G.; Ooi, B. 2018. "Untangling Blockchain: A Data Processing View of Blockchain Systems"

- Narayanan, Arvind; Bonneau, Joseph; Felten, Edward; Miller, Andrew; Goldfeder, Steven. 2016. "Blockchain". Investopedia. Archived from the original on 23 March 2016.

- Bentov I., Gabizon A., Mizrahi A. 2014. "Cryptocurrencies without proof of work". CoRR, abs/1406.5694