로또포엘

Lotto PoWL

Whitepaper

ver 1.42

2022 년 3 월 26 일

(최초: 2022 년 1 월 8 일)

차례

1. 로또포엘 소개

로또포엘(Lotto PoWL[1])은 로또 당첨 확률을 높이기 위해 기존 시스템에서 제공하는 '의사난수(Pseudo Random)' 방식을 배제하고, 기술적으로 더 혁신적인 '채굴난수(Mining Random)' 방식을 도입한 시스템입니다.

로또포엘은 세계최초 PoWL 방식의 로또번호 채굴시스템으로 채굴을 수행하면 로또번호와 채굴에 대한 보상으로 로또포엘 코인이 동시에 생성됩니다.

- PoWL = Proof of Work and Lotto
- PoWL 방식을 사용하여 로또번호를 생성합니다.
- PoWL 채굴에 대한 보상으로 로또포엘 코인을 제공합니다.

로또포엘 코인은 2종류로 발행됩니다. 프라이빗(중앙화) 블록체인 기반에서 운영되는 채굴코인과 퍼블릭(탈중앙화) 블록체인 기반에서 운영되는 매매코인으로 발행됩니다. 전자는 로또포엘 채굴시스템에서 보상용도로 사용되고 후자는 가상화폐 거래소에 상장되어 매매용도로 사용됩니다. 가상화폐 거래소 상장 코인은 ERC20토큰으로 발행될 예정입니다. ERC20토큰으로 발행된 로또포엘 코인은 다양한 이더리움 지갑에서 편리하고 안전하게 사용될 수 있습니다.

추후 로또포엘이 가상화폐 거래소에 상장되면, 채굴된 코인을 상장 코인으로 1:1 스왑해 드립니다.

2. 로또포엘 배경

로또포엘 프로젝트를 시작하게 된 계기는 우연한 기회에 '채굴방식'의 난수 생성 알고리즘(PoWL Algorithm)을 발견한 것입니다. 이는 정말 대단한 발견이었습니다.

원래 채굴이라는 행위는 블록체인을 만드는 과정에서 필수적으로 수반되는 과정인데, 단순히 코인만 나오는 것이 아니라 로또번호까지 나오게 되니 정말 일석이조입니다.

---

[1] PoWL: PoW와 Lotto의 합성어로 PoW(작업증명) 기술을 로또번호 채굴에 사용하는 혁신적인 채굴방식입니다.

앞으로 더 많은 연구가 필요하겠지만, 기존 '의사난수(Pseudo Random)' 기반의 난수함수보다 더 강력한 난수를 발생할 것으로 보입니다. 그만큼 PoWL 방식의 로또번호가 당첨될 확률이 높아지지 않을까 생각합니다.

대한민국에서 발행하는 로또는 45개 숫자 중 6개의 숫자를 맞추는 방식(로또 6/45)으로 현재 복권위원회[2]에서 복권 업무를 수행하고 있습니다. 로또의 당첨 확률은 다음과 같습니다.

순위	당첨 내용	당첨 확률	당첨금 배분 비율	기대 당첨금
1	6 개 번호 일치	1/8,145,060	총 당첨금의 75% (4 등과 5 등 금액 제외)	1,952,160,000 원
2	5 개 번호 + 보너스번호 일치	1/1,357,510	총 당첨금의 12.5% (4 등과 5 등 금액 제외)	54,226,666 원
3	5 개 번호 일치	1/35,724	총 당첨금의 12.5% (4 등과 5 등 금액 제외)	1,427,017 원
4	4 개 번호 일치	1/733	50,000 원	50,000 원
5	3 개 번호 일치	1/45	5,000 원	5,000 원

로또 6/45의 1등 당첨 확률을 계산하는 수식은 다음과 같다.

$$\binom{45}{6} = \frac{45!}{6!\,(45-6)!} = \frac{45 \times 44 \times 43 \times 42 \times 41 \times 40}{6 \times 5 \times 4 \times 3 \times 2 \times 1} = \frac{1}{8145060}$$

$$\approx 1.227 \times 10^{-7} = 0.0000122774$$

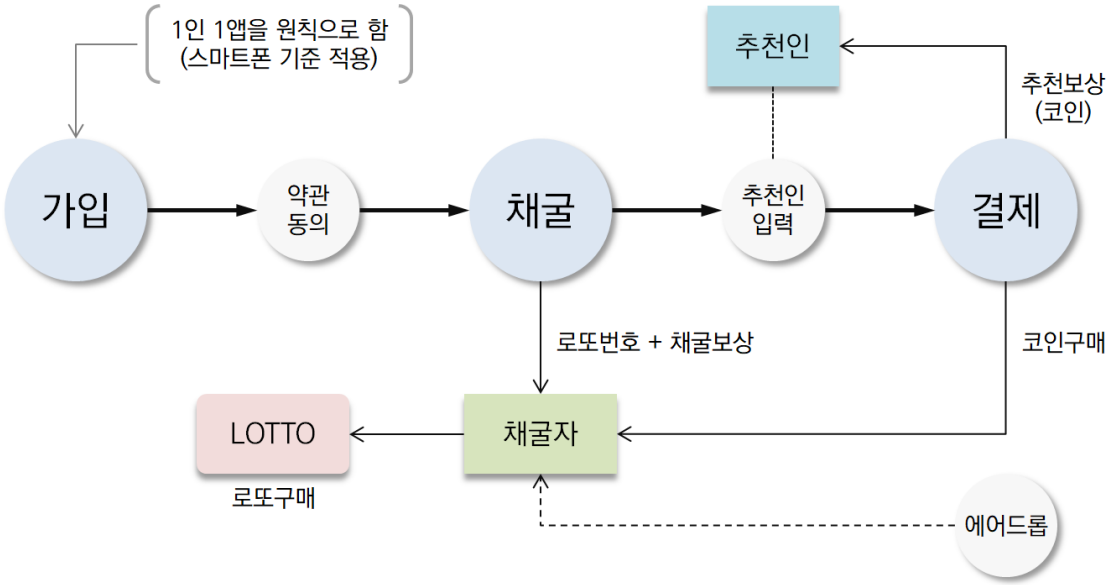
참고로 복권위원회의 복권사업 현황에 의하면, 복권 판매액에서 당첨금과 발행 경비를 제외한 수익금은 판매액의 약 41% 수준이라고 합니다. 복권 판매를 통해 조성된 기금은 대부분 저소득층 주거 안정 및 장학사업 등 취약계층 지원에 활용되어 사회 안전망 구축에 결정적 역할을 하고 있다고 볼 수 있습니다.

---

[2] 복권위원회: (福券委員會, Korea Lottery Commission, 약칭: 복권위, KLC), 복권의 발행, 관리, 판매, 복권 수익금의 배분, 사용 등에 관한 업무를 수행하는 대한민국 기획재정부의 소속기관이다.

3. 로또포엘 흐름도

로또포엘은 지갑과 채굴 기능을 합친 로또포엘 지갑을 제공하며, 이 지갑을 통하여 로또번호 채굴을 수행하게 됩니다. 그 과정은 다음과 같습니다.



로또포엘 지갑은 1인 1지갑을 원칙으로 합니다. 로또포엘 지갑을 다운로드 받아 설치 후 가입을 합니다. 가입이 완료되면 채굴을 시작할 수 있습니다. 채굴을 수행하면 로또번호와 코인을 보상으로 받게 됩니다. 로또번호는 6개 번호 조합으로 채굴됩니다.

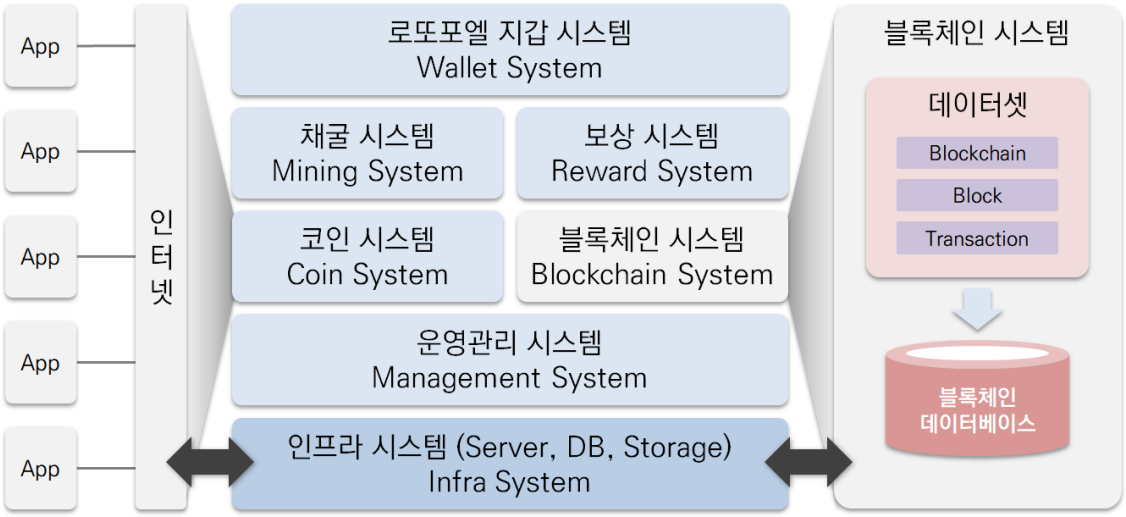
1일 채굴에 따른 보상량은 최대 한도가 정해져 있으며, 그 이상으로 채굴을 수행해도 보상이 나오지 않습니다. 이러한 결정은 채굴정책 및 코인정책 등에 따라 결정되어 공정하게 운영됩니다.

회원은 채굴 수행을 통하여 로또포엘 코인을 획득할 수 있지만, 추가적으로 코인을 구매할 수도 있습니다. 코인 구매 요청 시 추천인을 함께 입력하면, 그 추천인에게 구매금액의 일부를 판매(영업)에 대한 보상으로 코인을 지급하는 추천보상 제도를 운영할 예정입니다.

4. 로또포엘 시스템

로또포엘 시스템에 사용되는 블록체인은 프라이빗 블록체인을 사용합니다. 프라이빗 블록체인은 퍼블릭 블록체인에 비하여 더 적은 비용, 더 적은 리소스로 블록체인을 구현할 수 있는 장점이 있으며, 실제로 로또포엘 비즈니스에 매우 적합합니다.

로또포엘의 개발팀은 가상화폐 및 블록체인 유경험 개발자로 이루어져 있습니다. 개발언어는 JAVA 및 JSP를 사용합니다.



로또포엘 시스템은 크게 지갑 시스템, 채굴 시스템, 보상 시스템, 코인 시스템, 블록체인 시스템, 운영관리 시스템으로 구성됩니다.

- 로또포엘 지갑 시스템
  로또포엘 지갑은 보유 코인 정보 및 코인 전송(보내기 및 받기)이 가능하고, 채굴에 따른 보상을 즉시 확인할 수 있습니다.

- 로또포엘 채굴 시스템
  PoWL 알고리즘을 사용하여 로또번호를 채굴합니다. 기존 난수방식의 알고리즘이 아닌 수학적으로 견고한 채굴 알고리즘을 사용합니다.

- 로또포엘 보상 시스템
  로또포엘은 보상시스템을 통하여 채굴, 추천에 대한 보상을 제공합니다. 추천보상은 금전 보상을 기준으로 합니다..

- 로또포엘 코인 시스템

로또포엘은 코인의 보내기 및 받기 뿐만 아니라 잘못된 지갑주소로 인한 코인의 회수 기능을 포함하고 있어 매우 안전합니다.

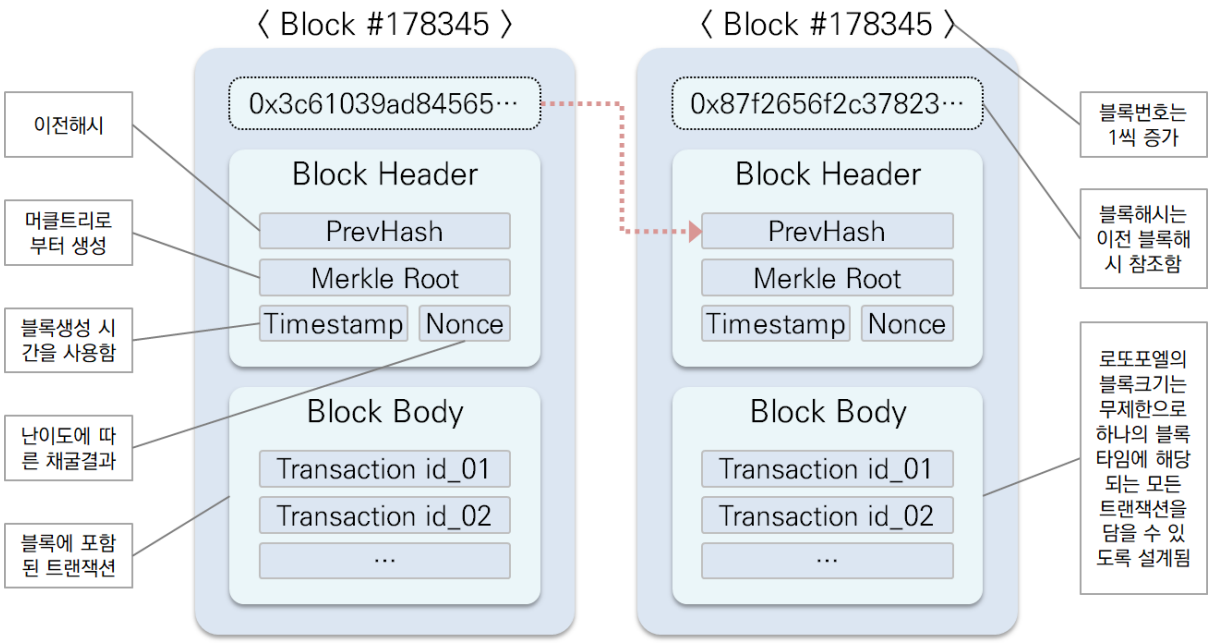
- 로또포엘 블록체인 시스템
  로또포엘은 모든 거래를 자체 블록체인에 저장하여 높은 신뢰성과 안정성을 보장합니다.

- 로또포엘 운영관리 시스템
  로또포엘은 투명한 회원관리 및 신속한 고객지원 등 운영관리를 위해 별도 관리 시스템을 구축합니다.

5. 로또포엘 블록체인 기술

로또포엘은 프라이빗 블록체인을 사용하며 채굴방식은 PoW과 PoWL를 사용합니다. PoW는 로또포엘 지갑에서 발생하는 코인전송에 의한 모든 트랜잭션을 블록체인에 쌓기 위해 사용되며, 스마트폰에서 PoWL은 로또번호 채굴 및 그에 따른 보상을 위해 사용됩니다.

다음은 로또포엘의 프라이빗 블록체인에 사용되는 블록체인 개념도입니다.



로또포엘의 블록체인 특징은 비트코인 블록체인과 개념은 동일하나 실제 구현은 로또포엘 프로젝트에 적합하도록 퍼블릭 블록체인이 아닌 프라이빗 블록체인으로 기능을 재해석하여

JAVA 및 JSP로 구현하였습니다. 프라이빗 블록체인으로 구현된 로또포엘은 퍼블릭 블록체인에 비해 보안이 대단히 강력합니다.

로또포엘의 기술적인 특징으로는 블록에 담을 수 있는 트랜잭션의 제한을 없앴다는 것입니다. 이렇게 되면 하나의 블록에 모든 트랜잭션을 담을 수 있으므로 비트코인처럼 트랜잭션 적체 현상이 절대 발생하지 않습니다.

6. 로또포엘 코인스펙

로또포엘의 코인스펙은 다음과 같습니다.

코인이름	로또포엘(Lotto PoWL)
코인심볼(티커)	LOT
발행목적	로또코인 사업 및 상장
블록체인	프라이빗 블록체인
총발행량	4,786,000,000 개 (약 47 억개)
채굴량	최대 25 개/일 이내 (채굴정책에 따라 변경)
채굴기간	48 개월 (채굴기간이후 채굴보상 없음)
반감기	12 개월 (52,560 블록, 현재기준)
합의알고리즘	PoW (블록체인 채굴), PoWL (로또번호채굴)
해시	SHA256
블록타임	PoWL: 60 초 이내, PoW: 600 초 (10 분)
블록크기	제한없음
채굴지갑	안드로이드 및 아이폰 (아이폰은 추후지원)
개발언어	JAVA, JSP, JavaScript
상장코인	ERC20 기반 (상장 거래소에서 스왑 실시)
상장거래소	국내 원화 거래소(2023 년 상장목표)

로또포엘 코인이 상장되면 거래소에서 채굴된 코인이 자동으로 상장용 코인으로 스왑을 실시하며, 이렇게 스왑된 로또포엘 코인은 다양한 이더리움 지갑(메타마스크, 마이이더월렛, 트러스트, 코이노미, 잭스 등)으로 전송하실 수 있습니다.

7. 로또포엘 로드맵

로또포엘 로드맵은 다음과 같습니다.

- 2022년 1월 ~ 3월
  사업기획 (프로젝트 방향 설정)
  홈페이지 제작 및 코인백서 작성
  개발팀 구성 및 개발기획

- 2022년 4월 ~ 9월
  (개발1팀)
  블록체인 시스템 개발
  코인 시스템 개발
  지갑 시스템 개발

  (개발2팀)
  채굴 시스템 개발
  보상 시스템 개발
  운영관리 시스템 개발

- 2022년 10월 ~ 2023년 5월
  로또포엘 서비스 출시 및 마케팅 시작

- 2023년 6월 ~ 10월 (예정)
  로또포엘 원화 거래소 상장 및 상장코인 스왑

8. 로또포엘 운영정책 변경

로또포엘의 정책은 로또포엘 운영회사에서 결정하게 되며, 1개월 또는 1년 주기로 변경될 수 있습니다. 변경 발생 시 회원에게 로또포엘 웹사이트 또는 로또포엘 지갑을 통해 정책변경 사항을 전달할 것입니다.

로또포엘의 정책변경에는 회원정책, 코인정책, 채굴정책, 보상정책, 비용정책 등이 포함될 수 있으며, 상세 내용은 다음과 같습니다.

① 회원정책 : 회원 등급이 현재 비회원 및 정회원으로 이루어진 2단계에서 더 세분화 될 수 있음
② 코인정책 : 총채굴량, 선채굴량, 채굴기간, 채굴 알고리즘, 블록타임, 반감기 등이 변경될 수 있음
③ 채굴정책 : 회원 등급에 따른 채굴량이 변경될 수 있음
④ 보상정책 : 회원 등급에 따라 추천보상 및 에어드롭 등이 변경될 수 있음
⑤ 비용정책 : 회원 등급에 따라 결제 비용 및 수수료 등이 변경될 수 있음

로또포엘의 정책변경은 로또포엘 시스템의 효율증대 및 암호화폐 가치증대 등을 목적으로 시행됩니다. 이러한 정책변경은 회원의 동의 없이 결정될 수 있습니다.

참고로 로또포엘의 가격은 로또포엘 지갑에 기준가격이 명시되어 있지만, 이러한 기준가격은 상장전까지는 운영회사 내부에서 회의를 거쳐 임의로 정한 것에 불과합니다. 따라서 회원은 이를 인지하여야 하며 이로인한 간접적 및 직접적 피해를 최소화하거나 예방해야 합니다. 만약 회원에게 이러한 피해가 발생하더라도 로또포엘 운영회사는 이에 대한 책임을 절대 지지 않습니다. 그러므로 로또포엘 회원은 항상 로또포엘 정책변경에 대하여 관심을 갖는 것이 필요합니다.

9. 로또포엘 운영정책

최종 수정일 : 2022년 3월 6일
로또포엘은 Republic of Korea 대한민국에 있는 회사입니다.

운영정책의 중요성
로또포엘 운영정책은 매우 중요합니다. 귀하가 로또포엘 서비스를 이용한다는 것은 우리의 운영정책(약관 포함)에 동의하는 것으로 간주됩니다. 본 운영정책은 귀하가 서비스(앱 포함)로 할 수 있는 것과 할 수 없는 것, 귀하의 권리와 책임, 그리고 로또포엘의 권리와 책임이 무엇인지 규정하기 때문에 이 운영정책을 이해하는 것이 중요합니다.

로또포엘은 수시로 본 운영정책(약관, 계약 포함)을 개정합니다. 이 페이지를 자주 확인하여 운영정책의 변경 사항이나 업데이트 사항을 인지하고 있는지 확인하십시오. 로또포엘 운영정책 또는 개정된 내용에 동의하지 않는 경우 로또포엘 사용을 중단해야 합니다.

운영정책 동의
귀하의 로또포엘의 운영정책(약관, 계약 포함)에 대한 동의는 로또포엘 서비스(앱 포함) 사용에 따른 최초 가입 또는 재가입 시 이루어 집니다. 이러한 귀하의 동의는 로또포엘 운영정책 전체를 읽고 이해했으며 이러한 운영정책에 구속되는 데 동의한 것으로 인정됩니다.

또한 귀하의 로또포엘의 운영정책(약관, 계약 포함)에 대한 동의는 로또포엘과 귀하 사이의 이해 및 계약에 대한 완전하고 배타적인 진술이며 주제에 대한 이전의 모든 구두 또는 서면 통신 관계를 대체합니다.

책임의 제한
어떠한 경우에도 로또포엘, 그 임원, 이사, 주주, 직원, 대리인, 계약자 및 제3자 기여자는 특별, 간접, 부수적, 결과적, 모범적 또는 서비스 또는 콘텐츠(사용자 제출물 포함)의 사용 또는 사용 불능으로 인해 발생하는 이익, 저축, 수익, 영업권, 사용, 데이터 또는 기타 무형 손실을 포함하되 이에 국한되지 않는 징벌적 손해, 로또포엘과 그 파트너가 그러한 손해의 가능성에 대해 조언을 받았더라도 계약, 과실 또는 불법 행위에서 법이 허용하는 한도 내에서 묵시적 보증을 포함하여 본 약관에 따른 청구에 대한 로또포엘 및 그 파트너의 책임 또는 기여는 100달러($100) 또는 귀하가 서비스를 사용하기 위해 지불한 금액에서 로또포엘이 취한 이득에 해당하는 금액 또는 그 이하로 제한됩니다.

계정 해지 또는 취소
로또포엘은 단독 재량으로 사전 통지 없이 언제든지 서비스(앱 사용 포함) 또는 귀하의 서비

스 사용을 일시적으로 중단하거나 영구적으로 중단할 수 있습니다. 서비스가 일시 중단되거나 중단되면 본 계약(약관 포함)에 의해 부여된 권리가 자동으로 종료되거나 해제되며 더 이상 액세스할 수 없습니다. 또한 언제든지 계정을 취소할 수도 있습니다.

로또포엘은 서비스 또는 귀하의 계정이 정지 또는 종료된 결과로 귀하가 입을 수 있는 손해, 손실 또는 기타 결과에 대해 책임을 지지 않습니다.

귀하는 로또포엘의 명시적인 사전 서면 동의 없이 본 운영정책(약관, 계약 포함)에 따른 귀하의 권리를 양도할 수 없습니다. 그러한 동의가 없는 경우 양도 시도는 무효입니다.

보증 부인

귀하는 서비스(앱 포함) 사용에 따른 위험 부담이 전적으로 귀하에게 있음에 명시적으로 동의합니다.
우리는 운영정책(약관, 계약 포함)에서 허용하는 최대한의 범위 내에서 명시적이든 묵시적이든 어떠한 종류의 보증 없이 “있는 그대로” 제공됩니다. 이러한 보증에는 상품성, 특정 목적에의 적합성, 소유권 및 재산권 비침해에 대한 묵시적 보증이 포함되지만 이에 국한되지 않습니다.

또한, 로또포엘은 서비스(앱 포함), 콘텐츠, 그 특징 및 기능이 귀하의 특정 요구 사항을 충족하고, 중단되지 않고, 안전하고, 정확하고, 완전하고, 오류, 바이러스 또는 기타 유해한 구성 요소가 없음을 보증하지 않으며 로또포엘은 그러한 불일치를 수정한다고 보증하지 않습니다. 또한 귀하는 로또포엘 서비스의 품질 및 성능에 대한 모든 위험을 감수하는 것으로 동의합니다.

준거법

본 운영정책(약관, 계약 포함)은 법률 원칙의 충돌에 관계없이 로또포엘의 본사가 속한 해당 국가의 법률을 적용 받고 이에 따라 해석됩니다. 본 운영정책으로 인해 발생하거나 본 운영정책과 관련하여 발생하는 모든 분쟁 또는 논쟁은 해당 국가의 법원의 배타적 관할권 및 재판지의 적용을 받습니다. 귀하는 이러한 법원의 인적 관할권 및 재판지에 동의합니다.

법원에서 불법, 무효 또는 집행 불가능한 것으로 판명된 모든 조항은 자동으로 법률의 최소 요구 사항을 준수하는 것으로 간주되며 다른 모든 조항과 함께 완전한 효력을 발휘합니다. 한 가지 경우에 조항을 포기한다고 해서 향후에 해당 조항의 시행이 금지되는 것은 아닙니다. 여기에 있는 하나 이상의 조항에 대한 불법, 무효 및/또는 시행 불가능에 대한 그러한 발견은 나머지 조항에 영향을 미치지 않습니다.

일방 당사자가 본 운영정책(약관, 계약 포함)의 조항 또는 그에 따른 조항의 집행을 위해 소송, 소송 또는 기타 절차를 진행해야 하는 경우, 각 당사자는 변호사 및 전문 전문가 비용을 포함하여 각자의 비용과 경비를 부담해야 합니다.

10. 로또포엘 면책조항

로또포엘 백서에서 제공되는 로또포엘 프로젝트 관련 정보와 자료는 미래에 대한 정보제공의 목적만을 가지며, 금융자문 또는 법률자문으로 간주하여서는 안 됩니다. 개인은 각자의 필요에 따라 최선을 판단하기 위해 해당전문가와 상담해야 합니다.

로또포엘 백서는 로또포엘 프로젝트에 관하여 어떠한 결과에 대해서 보장이나 약속을 하지 않습니다. 특히 로또포엘 암호화폐 가치는 상장 전이나 상장 후 모두 높은 변동성으로 인해 로또포엘 암호화폐의 가치가 폭락할 가능성이 높습니다. 이로 인하여 로또포엘 암호화폐 보유자는 이를 인지하여야 합니다. 누구든 먼저 자신의 금융자문인과 상담하고 본인이 직접 조사와 검토를 마친 후에 결정해야 합니다.

로또포엘 운영회사는 법적으로 최대 허용하는 범위 안에서 특정 평론, 정보, 견해, 조언, 분석 및 추천의 내용이 부정확, 불완전 또는 신뢰할 수 없는 것으로 판명되거나, 이로써 경제적 손해가 초래되어도 법적 책임을 지지 않습니다.

로또포엘의 웹사이트나 관련 웹사이트, 또는 온•오프라인 소셜 미디어 채널을 통해 제공된 내용은 법률적 조언이나 자문이 아니며, 변호사의 의뢰인 비밀유지 관계도 형성되지 않습니다. 또한, 로또포엘 백서는 계약서 또는 약정이 아니며 회사의 재량에 따라 언제든지 변경되거나 업데이트가 될 수 있다는 사실을 유의하여야 합니다.

로또포엘 웹사이트의 정보나 링크된 자료를 사용하는 경우, 모든 위험은 사용자가 부담해야 합니다. 다시 말해 로또포엘 운영회사는 직접적 혹은 간접적으로 로또포엘 백서로 인하여 손실이 발생하는 것에 대해 어떠한 책임도 지지 않습니다.

11. 참고문헌

1. Alt chains and atomic transfers: https://bitcointalk.org/index.php?topic=193281.msg2224949#msg2224949/
2. Bitcoin whitepaper: http://bitcoin.org/bitcoin.pdf/
3. Decentralized autonomous corporations, Bitcoin Magazine: http://bitcoinmagazine.com/7050/bootstrappinga-decentralized-autonomous-corporation-part-i/
4. Decentralized autonomous corporations, Bitcoin Magazine: https://tinyurl.com/Bootstrapping-DACs/
5. Ethereum Merkle Patricia trees: https://github.com/ethereum/wiki/wiki/%5BEnglish%5D-Patricia-Tree/
6. Ethereum RLP: https://github.com/ethereum/wiki/wiki/%5BEnglish%5D-RLP/
7. Intrinsic value: http://bitcoinmagazine.com/8640/an-exploration-of-intrinsic-value-what-it-is-whybitcoin-doesnt-have-it-and-why-bitcoin-does-have-it/
8. Joseph Poon and Tadge Dryja, Lightning Network: https://lightning.network/lightning-network-paper.pdf/
9. Mastercoin whitepaper: https://github.com/mastercoin-MSC/spec/
10. Merkle trees: http://en.wikipedia.org/wiki/Merkle_tree/
11. Mike Hearn on Smart Property at Turing Festival: http://www.youtube.com/watch?v=Pu4PAMFPo5Y/
12. Peter Todd on Merkle sum trees: http://sourceforge.net/p/bitcoin/mailman/message/31709140/
13. Reusable proofs of work: http://www.finney.org/~hal/rpow/
14. Secure property titles with owner authority: http://szabo.best.vwh.net/securetitle.html/
15. Simplified payment verification: https://en.bitcoin.it/wiki/Scalability#Simplifiedpaymentverification/
16. Smart contracts: https://en.bitcoin.it/wiki/Contracts/
17. StorJ and Autonomous Agents, Jeff Garzik: http://garzikrants.blogspot.ca/2013/01/storj-and-bitcoinautonomous-agents.html/
18. The Simple Two Way Peg: http://www.truthcoin.info/blog/drivechain/