BLACKPEARL.CHAIN 백서

[page 1]

[page 2]

1. 개요

블록체인이란 데이터 블록들을 부정 조작할 수 없도록 암호로 보장되어 있는 체인 형태의 데이터 구조로 결합한 탈중앙 분산 거래 원장입니다. 기존의 중앙 집권화된 데이터 베이스와는 다르게, 블록체인은 공정하며, 투명하고, 부정 조작을 할 수 없습니다. 바로 이런 특성 덕분에, 블록체인은 테크놀로지 및 경제 분야에서 무한한 잠재력을 가지고 있습니다. 블록체인은 거의 모든 산업에서 사용될 수 있으며, 인터넷 혁신을 뒤잇는 차세대 기술 혁신입니다.

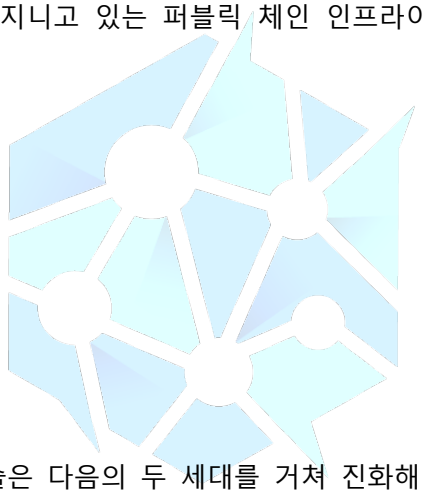
비트코인과 같은 디지털 암호화폐의 발전으로, 블록체인 기술은 큰 주목을 끌었습니다. 블록체인 기술은 분산화된 합의이며, 데이터 암호화, 컨센서스(합의) 알고리즘 및 경제적 지원을 통해 노드 간의 상호 신뢰 없이 point-to-point 거래가 가능합니다.

이더리움의 스마트 컨트랙트를 지원하는 블록체인의 도입은 블록체인 적용의 발전에 새로운 기회를 창조해 왔습니다. 블록체인 시스템의 신뢰된 실행 환경에 기반하여, 스마트 컨트랙트 플랫폼은 블록체인의 다양한 디지털 자산 운용을 가능하게 하며, 풍부한 탈중앙화 애플리케이션(DApp)에 접근할 수 있도록 해줍니다. 디지털 화폐 거래 시스템과 스마트 컨트랙트 애플리케이션의 발전은 블록체인의 고성능과 확장성을 필요로 합니다. 그러나, 현재 주류 퍼블릭 블록체인 시스템은 낮은 성능을 가지고 있고 비용이 높은 반면에 빠르고 효율적인 서비스와 긍정적인 사용자 경험을 제공할 수 없습니다.

블록체인 기술은 기술적 그리고 경제적인 면 모두의 각계 각층에 엄청난 가치가 될 수 있습니다. 신뢰에 대한 필요성이 있는 한, 블록체인 기술은 저가의 비용과 고효율성으로 신뢰를 구축하는데 사용될 수 있을 것입니다.

블록체인 기술은 생산 관계를 변화시켜 왔습니다. 수 천년 동안, 거래 보안은 은행, 보험사, 알리페이, 부동산 중개업자 등과 같은 신뢰할만한 제 3의 중개자들에 의해 보장되어 왔습니다. 이제 우리는 제 3자 중개자 없이도 P2P(Peer-to-peer) 방법의 블록체인 기술을 통해 매우 저렴한 비용과 더욱 높은 효율성으로 완전한 거래를 할 수 있습니다.

블록체인 시장은 수 조(兆) 달러에 달하는 시장입니다. 생산 관계와 비즈니스 모델이 엄청난 변화를 겪어 왔습니다. 중앙화 된 서버들은 기존의 인터넷 기반 중앙화 모델을 기반으로 한 큰 가치를 가지고 있습니다. 그러나, 블록체인 생태계에서 가장 가치 있는 자산은 거대한 데이터, 거래 그리고 비즈니스 활동을 지니고 있는 퍼블릭 체인 인프라이며, 퍼블릭 체인에는 큰 상업적 가치가 있습니다.



지난 십여 년간, 블록체인 기술은 다음의 두 세대를 거쳐 진화해 왔습니다.

비트코인이 대표하는 첫 번째 블록체인 디지털 화폐 시대:

2008년 10월 31일, 비트코인 창시자 나카모토 사토시(가명)는 암호화 메일 그룹에 “비트코인: P2P 전자 화폐 시스템” 이라는 문서를 출판했습니다. 블록체인 기술은 비트코인 작동을 지원하는 핵심 기반이었습니다. 비트코인은 십년 간 안전하게 작동하는 데 어떤 제 3자 신탁 중개자도 필요로 하지 않았으며, 이는 블록체인 기반 기술이 친숙하지 않는 두 명의 개인 간 신뢰를 P2P 방식으로 구축하고 거래를 안전하게 할 수 있다는 것을 증명하였습니다. 탈중앙화 기계 신뢰는 시간과 해킹이라는 시험을 모두 견뎌냈습니다.

이더리움이 대표하는 두 번째 블록체인 기술 세대:

2013년, 이더리움에 의해 제안된 스마트 컨트랙트를 지원하는 블록체인 시스템은 블록체인 적용의 발전을 위한 새로운 기회를 만들어 냈습니다. 이더리움은 블록체인 기술을 기반으로 한 신뢰된 실행 환경을 도입했습니다. 스마트 컨트랙트는 복잡한 작업을 수행하고 풍부한 탈중앙화 애플리케이션(DApp)을 실현하기 위해 다양한 블록체인 디지털 자산들을 관리할 수 있습니다. 이와 같은 혁신은 블록체인 기술을 기반으로 다수의 상업 애플리케이션이 실행될 수 있도록 합니다.

현재, 블록체인 산업은 어떠한 긍정적인 퍼블릭 체인 3세대가 없다는 딜레마에 직면하고 있습니다. 지금까지 발표된 대부분의 퍼블릭 체인들은 “Impossible triangle”이라고 불리는 해결 불가능한 세 가지: 보안, 탈중앙화, 그리고 성능을 해결하는 데에 실패했습니다. 퍼블릭 체인 1세대, 2세대들은 아직 프로토타입 단계에 있으며 대규모 상업 애플리케이션을 위한 기반을 가지고 있지 않습니다.

주요 문제점:

주류 퍼블릭 체인들의 성능은 낮습니다. 비트코인의 TPS는 7까지만 도달할 수 있습니다. 이더리움의 TPS는 10-20까지이며 거래가 종종 막히거나 상업 수준의 니즈를 충족할 수 없습니다.

비용은 매우 높으며, 거래 비용은 보통 대부분 산업의 이익 한도를 초과하며 다양한 산업에 적용이 제한되어 블록체인의 가치를 실현할 수 없습니다.

거래 확정은 매우 느리게 진행되며 즉각적인 서비스나 좋은 사용자 경험을 제공하지 않습니다. 결제에 관련해서, 비트코인 결제는 완료되기까지 1시간이 소요되며, 혼잡이 발생할 경우에는 하루까지 걸릴 수도 있습니다. 온라인 판매 업체들에 인하여 상품과 서비스 구입 결제를 이만큼 기다린다는 것은 용납할 수 없는 일입니다.

퍼블릭 체인 비교

	블록 생산 시간	TPS	컨센서스(합의) 알고리즘	탈중앙화 레벨
ETH이더리움	15초	7	POW작업증명	채굴 중앙화
EOS이오스	0.5초	28	DPOS위임된 지분증명	대표 중앙화
Gongxinbao 공신바오	3초	<1	POCS	동맹 체인
NEO네오	10초	<1	DBFT 위임된 비잔틴 장애 허용	컨센서스 노드 중앙화
Qtum퀀텀	1분-4분	<1	POS지분증명	거대 자본 소유주들에 의한 중앙화 권리
Bytom 바이텀	30초-7분	<1	POW 작업증명	채굴 중앙화
ONT 온톨로지	1초-15초	<1	VBFT(Verifiable Byzantine Fault Tolerance) 검증 가능한 비잔틴 장애 허용	대자본 관리 및 자본 중앙화
ADA에이다	20초	<1	POS 지분증명	대자본 소유주 및 지역 중앙화 권리

블록체인 산업의 이상적인 제3세대 퍼블릭 체인의 공개가 이루어지지 않았기 때문에, 과도기 동안 “3세대 퍼블릭 체인”이라고 불리는 체인들이 나타나기 시작했습니다. 그러나, 이들은 본질적으로 동맹 체인에 속해있으며, 특정한 성능 향상을 얻기 위해 보안을 희생하고, 본질은 이 역시 해결 불가능한 3가지 요소들, “impossible triangle”을 돌파하지 못했습니다. 이러한 동맹 체인들은 오버 프로비저닝(over-provisioning) 설계에 속해 있어야 합니다. 소량의 수퍼노드들은 큰 리스크를 가지고 있으며, 완전히 분산화 될 수 없습니다. 부정적인 조작이 일어나게 되면, 사용자 자산에 손실을 입힐 뿐만 아니라 전체 체인의 신뢰성이 손상됩니다. 또한, 퍼블릭 체인들의 신뢰 상실은 실제로 블록체인 산업 전체에 엄청난 부정적인 영향을 끼칠 수 있습니다.

블록체인 산업 전체의 발전은 블록체인 기술의 진정한 돌파구가 될, “impossible triangle” 의 솔루션, 즉 거래 비용 절감에 달려있습니다. 이 발전이 일어나야만 블록체인 기술은 대규모 수준에 도달할 수 있을 것입니다.

여기서 우리는 BlackPearl.Chain 주식회사가 개발한 BlackPearl.Chain을 소개합니다.

BlackPearl.Chain 전체가 근본적으로 철저히 개발되었습니다. BlackPearl.Chain은 비트코인, 이더리움이나 다른 퍼블릭 체인 모델과는 완전히 다릅니다. BlackPearl.Chain은 “impossible triangle”을 해결해 왔습니다. BlackPearl.Chain 은 VRF lightning fast(번개 속도) 컨센서스, 3계층 샤딩(sharding) 기술, 임계값 암호화, 슈퍼 시크릿 프라이빗 키, 다차원 라우팅(routing), IPFS 스토리지, 시스템 계약, 그리고 뉴런 노드 관리를 통해 탁월한 성능을 실현합니다.

BlackPearl.Chain은 넓은 범위의 산업 애플리케이션이 블록체인 산업에 정착할 수 있게 돕기 위하여 대규모 상업 애플리케이션을 매우 낮은 수수료(gas fee)
로 실행할 수 있게 합니다.

2. BlackPearl.Chain 기술 돌파구

BlackPearl.Chain은 다량의 실시간 소액 결제, 탈중앙화 디지털 화폐 거래, 실시간 메시지, 전자상거래, 검색, 공증, 소셜 미디어, 디지털 자산, 추적 가능성 등을 효과적으로 지원할 수 있습니다.

BlackPearl.Chain은 선팽창 기능으로 완전히 분산되며, 수 천만의 TPS를 노드의 증가로 지원할 수 있습니다. BlackPearl.Chain은 매우 안전하며, 양자 연산 및 생물학적 연산에 저항력을 가지고 있습니다.

BlackPearl.Chain은 컨센서스, 연산력, 스토리지 그리고 커뮤니케이션에 관한 혁신적인 돌파구를 만들어 왔습니다. BlackPearl.Chain은 확장이 가능하고, 증명할 수 있을 정도로 안전하며, 에너지 효율적입니다. 특히, BPChain은 다음과 같은 양상에서 돌파구를 만들었습니다.

● 지능적 샤딩으로 완전히 확장 가능: 혁신적인 3계층 샤딩 개발로 샤드 간 신뢰를 완전히 해결하였습니다. 또한 샤딩 컨센서스와 인터샤드 커뮤니케이션을 제공합니다. 인공지능 가능한 데이터 수집 및 분산의 부하 균형이 자동적으로 샤딩과 병합을 완료할 수 있습니다. 퍼블릭 체인의

성능은 이 해결책, 즉 BlackPearl.Chain의 성능을 중앙 서버의 성능보다 능가하게 하는 방법을 통해 무한히 발전할 수 있습니다.

● 안전하고 빠른 컨센서스(합의) : BlackPearl.Chain은 VRF lightning fast(번개 속도) 합의를 실행합니다. BlackPearl.Chain의 독보적인 VRF 실행은 현재 라운드의 투표 노드를 무작위로 선택하며, 선구적인 번개 속도 합의를 완수합니다. 합의가 완료되기까지는 0.3초-3초 정도의 시간만이 요구됩니다.

● 컴퓨터 파워 절약: BlackPearl.Chain에서, APP는 한 노드입니다. 이 기술은 전 세계의 IDLE 연산력과 대역폭을 완전히 조직하고 활용하며, 전문적인 채굴 기계에 대한 추가적인 큰 비용의 발생 없이 강력한 연산 및 스토리지 능력을 구축할 수 있게 해줍니다. 사용자는 합의에 참가하거나 블록 생산을 위해 BlackPearl.Chain 월렛을 설치할 수 있습니다.

● 향상된 네트워크 성능 : 슈퍼 라우팅 된 P2P 전파는 가정 광대역이 수 천 개의 싱글 샤드 TPS 실현하는 것을 가능하게 합니다. (현재 광대역 조건에서, 측정되는 TPS 최고점은 5730임)

프로토콜과 네트워크 계층을 혁신함으로써, BlackPearl.Chain은 세계적으로 떠오르고 있는 탈중앙화 경제를 지원할 수 있는 확장 가능하고 안전한 블록체인 시스템을 제공합니다. BlackPearl.Chain은 대량의 분산 교환, 상호 공정 게임, 비자(Visa) 규모의 결제 시스템, 그리고 사물 인터넷 거래를 포함으로, 이전까지 블록체인에서 실행 하지 못했던 애플리케이션을 가능하게 할 것입니다. BlackPearl.Chain은 수십억 인구의 신뢰를 구축하고 근본적으로 공정한 경제를 창조하기 위하여 최선을 다하고 있습니다.

3. 블록체인의 근본적인 도전과 BlackPearl.Chain의 접근

3.1 블록체인 역사 검토

블록체인 역사에 대해 간단히 검토해 보는 것은 BlackPearl.Chain의 혁신적인 본질을 이해하는데 도움이 될 것입니다.

2008년에, 나카모토는 “비트코인: P2P 전자 화폐 및 금 시스템” 이라는 유명한 문서를 출판했고, 2009년 1월에 Genesis 블록이 채굴되었습니다. “2009년 1월 3일 더 타임스지 헤드라인 - 영국 재무장관이 은행들을 위해 두 번째 구제금융을 준비한다.” 마치 마법처럼, 이와 함께 비트코인 블록체인의 시대가 시작되었습니다. 2013년에는 비트코인이 그 역사 중 가장 중요한 버전을 공개했습니다. 이 버전은 비트코인 노드의 내부 관리와 네트워크 커뮤니케이션을 최대로 활용하였으며, 디지털 화폐로서의 비트코인은 전 세계적으로 영향을 끼치기 시작했습니다. 비트코인은 첫 번째 암호 디지털 화폐로서 위대한 성공을 거뒀지만, 비트코인 확장성의 부족은 차후 블록체인의 적응을 매우 제한하게 되었습니다. 비트코인은 블록체인의 1.0 시대를 대표합니다. 비트코인의 확장성 문제를 해결하기 위해, 비탈릭 부테린(Vitalik Buterin)은 이더리움을 개발했습니다. 이더리움은 EVM 페이퍼에서 ICO 프레임워크까지, 각기 다른 버전들의 PO부터 2015 프론티어 단계까지, PoW의 메트로폴리스 단계에서 PoS의 세레니티 단계까지, 이더리움의 튜링 완전성, 스마트 계약 플랫폼, ASIC 디자인에 대한 저항성과 같은 명확한 디자인과 시스템 구조를 가지고 있으며 블록체인 2.0 시대의 주요 특징들입니다. 이더리움은 플랫폼 인터페이스와 개발자들이 차세대 분산 애플리케이션을 구축하고 출판할 수 있는 프로그래밍 언어를 제공합니다. 다음에 이어지는 이야기는 매우 유명한 것입니다. 2018년 2월, 비트코인 계산력은 20EH/s에 도달했으며, 깃허브(Github)에는 9만 개가 넘는 오픈 소스 프로젝트가 블록체인과 관련되어 있습니다. 중국, 미국, 영국, 싱가폴, 러시아, 일본, 대한민국을 포함한 90개가 넘는 국가들이 블록체인 기술에 대한 연구에 참여해오고 있습니다. 2008년부터 2018년까지, 블록체인에 대한 아이디어와 이론적 근거가 일반 대중에 의해 이해되고, 탐구되어지고, 실행되었습니다. 이 모든 것이 단 10년 안에 일어났습니다. 인터넷의 발전에 비교해 봤을 때 누구나 블록체인의 성공을 알아볼 수 있을 것입니다. 1974년, 미국 국방부 고등연구 소가 TCP / IP 프로토콜을 발표함으로써 인터넷 시대의 첫 번째 해를 기록했고, 20년이 지나 1994년에 중국이 인터넷 시대에 공식적으로 진입했습니다.

3.2 BlackPearl.Chain의 블록체인의 두 주요 과제에 대한 접근

3.2.1 SHD 완전성

분산 시스템에서는 일관성, 가용성, 그리고 파티션 허용은 동시에 가능하지 않습니다. 이는 CAP 정리라고 불립니다. 나카모토의 블록체인은 나카모토 합의라고 불리는 합의에 도달하기 위해 확률적으로 강력한 일관성에 의존합니다. 블록체인 시스템에서는 CAP 정리와 비슷하게, 보안(S), 고성능(H), 그리고 분산화(D)는 동시에 실현할 수 없습니다. 이는 SHD 완전성 문제라고 불립니다. CPU 동력이 불충분하다는 전제 아래, 나카모토는 고성능(H)이 희생되는 대신 보안(S)과 분산화(D)가 공존할 수 있다는 것을 증명했습니다. 합의 알고리즘과 각 블록의 수용성 디자인 때문에 비트코인에서 블록을 생성하는 데 평균 10분의 시간이 걸리고 1초에 7개의 거래만이 진행될 수 있습니다. 뿐만 아니라, 고성능의 "ASIC 채굴 기계"의 출현에 따라, 일반 CPU 컴퓨터 동력으로 비트코인에서 이득을 얻을 확률은 거의 0에 가깝게 줄어들었습니다. 채굴 기계는 쉽게 많은 이익을 얻을 수 있으며, 최근 채굴과 채굴 풀의 출현은 분산화의 핵심을 완전히 망가뜨렸으며, 이제 비트코인이 평등한 참여 커뮤니티가 아니라는 것은 명확합니다. 설상 가상으로, 채굴과 채굴 풀은 지속적으로 연산력을 독점하고 있습니다. 소량의 참여자가 결국 51%의 연산력을 소유하는 일이 결국 일어날 수 있으며, 보안(S)은 보장되지 않을 것입니다. 그러므로, 비트코인의 블록체인은 SHD의 균형을 잃었다고 볼 수 있습니다.

ASIC 채굴 기계의 파괴적인 영향을 피하기 위해, 이더리움은 ASIC 저항 알고리즘인 “캐시 반복 읽기” 를 적용했습니다. 이는 보안(S)과 분산화(D)를 빠른 시간 내에 유지보수 했습니다. 그러나, 이더리움의 첫 번째 대규모 스마트 컨트랙트 애플리케이션 “CryptoKitties”가 이더리움 시스템을 완전히 붕괴했으며 고성능(H)이 매우 낮습니다. 따라서, 최근의 컨센서스 트렌드는 PoS 혹은 DPoS에서 PoW로 변하고 있습니다. PoS 또는 DPoS 컨센서스로 전환한 블록체인 시스템은 시스템 성능은 매우 향상하였지만 분산화의 근본적인 의미를 무시했고, 시스템은 소수의 이해 당사자들에 의해 숙달되었으며 발전의 방향이 기존 중앙집권화 시스템과 다를 바 없는 것입니다.

VRF 기반 컨센서스 메커니즘을 개발함으로써, BlackPearl.Chain은 모든 토큰 홀더들이 권리와 이익을 소유하는 것이 보장되고, 동시에 보안과 고효율성을 향상시키고, 탈중앙화라는 토대 또한 유지하기 위하여 모든 노드가 참여 가능한 시스템을 채택합니다. 따라서, BlackPearl.Chain은 SHD 완전성을 실현했습니다.

3.2.2 평등한 가치 전송

인터넷의 시대는 정보 전달의 방법과 그 이론적 근거를 변화 시켰습니다. 사람들은 정보를 편리하고 저비용으로 전송하기 위해 인터넷 기술을 사용합니다. 인터넷은 기하급수적 수준의 효율성과 비용 감축을 실현하였고, 사람들은 전례 없는 새로운 상품 경험과 서비스를 얻고 있습니다. 그러나, 정보 전송의 개념과 가치 전송의 개념은 다릅니다. 인터넷 네트워크는 P2P 가치 전송 기능을 가지고 있지 않습니다. 가치 전송은 고유한 부기 기능을 보장해야 하기 때문에 부기 기능을 맡은 중앙 사무소에 의존합니다. 이는 정보 이전의 복제 가능성과 같지 않습니다. 분산 공유 회계 제도를 이용하여, 비트코인은 분산 신뢰를 설립하여 중앙집권화 조직에 더 이상 의존하지 않게 되었고, P2P 가치 전송을 지원하여 가치 전송과 가격 책정 규칙을 변경했습니다. 채굴 풀의 출현으로, 비트코인의 가치 전송은 점점 가라앉고 있고, 일반 참여자 및 채굴 기계 소유자에 의한 가치에 대한 접근성은 더이상 평등하지 않으며, 가치가 채굴 풀에 급속히 집중되고 있습니다. 이더리움은 ASIC 저항성 알고리즘을 통해 불평등에 저항하고 체인의 자원을 숨기기 위해 “Gas” 소비를 활용하여 채굴 기계의 가치 축적을 특정한 규모까지 지연시킵니다. 그러나, 우리는 이를

부정적이고 단기적인 계획이라고 간주하며, 블록체인 발전의 장기적 성장을 지원하기에는 부족하다고 생각합니다. PoS 혹은 DPoS 컨센서스는 PoW 연산력 독점을 파괴함으로써 평행을 찾으려 시도하지만 유력한 토큰 소유자들은 여전히 가치를 지향하며 중앙 집권화는 PoW보다 더 집중되어 있습니다. 현재 블록체인 및 암호화폐의 발전에 따라, 80 대 20의 법칙과 같이, 가치는 소수의 사람들에게만 집중됩니다.

BlackPearl.Chain 팀은 존재하는 가치 이전의 방법을 변화시키고, 가치가 완전히 개방적으로 유통되게 하고, 안정된 가치 이전 시스템을 사용자에게 제공하는 것을 목표로 합니다. BlackPearl.Chain 팀은 각 개인이 서비스의 제공자인 동시에 구매자가 될 수 있다고 믿습니다. 즉, 구매자인 동시에 판매자인 것입니다. 탈중앙화 시장의 핵심 가치는 가격 조정 메커니즘이며, 가격은 동적 평형 방식에 도달할 것입니다. BlackPearl.Chain은 가격 동력 변동을 연구하기 위해 평균 필드 게임 이론을 사용할 것입니다. 권리와 이익 간에는 긍정적인 상관성이 있을 것이나, 이는 평행적인 관계는 아니므로 힘의 초과적인 집중을 억제합니다. BlackPearl.Chain은 안정된 가치 상호 접속 시스템의 새로운 세대를 창조해 냈습니다. 이 시스템은 비즈니스 모델과 사회에 경제적으로 큰 혁신을 가져올 것입니다.

4. BlackPearl.Chain 개발자들

BlackPearl.Chain 개발자들과 빌더(builder)들은 최고의 인터넷 기업, 학교 그리고 연구 기관 출신입니다. 팀은 게임 이론을 블록체인에 통합한 수학자들로 구성되어 있으며, 커뮤니케이션 전문가, 컴퓨터 전문가, 경제 전문가 및 철학자들 역시 포함되어 있습니다. BlackPearl.Chain의 모든 이론적 설계는 두 차례의 확인 과정을 적용합니다. 첫 번째로, 수학자들이 컨센서스 모델링 및 수치 시뮬레이션을 완료합니다. 두 번째로, 컴퓨터 및 커뮤니케이션 전문가들이 BlackPearl.Chain 프로젝트의 이론적 디자인을 엄격한 기준에 따라 실제 검증합니다.

BlackPearl.Chain의 현재 작업 결과는 긴밀한 협력과 이론과 실험, 소프트웨어 및 하드웨어 간의 공동 노력 덕분에 이루어졌습니다. VRF 컨센서스 메커니즘은 수학, 커뮤니케이션 및 컴퓨터 분야의 전문가들에 의해 개발되었습니다.

주요 공헌자

Jack Liu 잭 리우: 중국 Chengzhou 대학교를 졸업하고, 다수의 소프트웨어 저작권 및 발명 특허를 가지고 있습니다. 국가 부처 및 위원회 관련 보안 컨설턴트로서 근무하였으며, OK코인 수석 과학자, Tencent 수석 개발자, 2010년 Tencent에 의해 매입된 베이징 Sun Moon Guanghua 소프트웨어 Co.의 창립자입니다.

상당한 기술신봉자로서, Liu씨는 외계 문명, 중력파, 단백질 구조 예측, 기후 변화 트렌드, 생명과학 및 암호 조사를 포함해 다양한 국가의 오픈 소스 프로젝트를 위한 대규모 분산 컴퓨팅 시스템에 참여해 왔습니다.

Sarah (Ping) Li는 하와이 대학교에서 물리학 석사를 마쳤습니다. 열정적인 기술 에반젤리스트(evangelist, 전도사)로서, 전 세계에 블록체인 기술을 홍보하기 위하여 노력해 왔습니다. NAND Flash 에반젤리스트이며, NAND Flash를 모바일 산업 벤더들과 주 운영 시스템으로 사용되도록 성공적인 홍보를 지속해 왔습니다.

Sarah는 소프트웨어 전문가이며, C언어와 NAND Flash시스템 소프트웨어, 다양한 내장형 OS, 스토리지 네트워크 프로토콜(USB, SATA, SCSI, NVME), 파일 시스템에 뛰어난 능력을 가지고 있습니다. 실리콘 밸리에서 20년이 넘게 일해오고 있으며, 애플, 소니, 삼성, 샌디스크에서 근무한 적이 있습니다.

Sarah는 샌디스크에서 기술 에반젤리스트 및 수석 연구원 직위에 있었으며, 마이크로소프트 윈도우즈 CE OS, Symbian OS에 NAND 플래시를 채택하도록 한 주 공헌자이자 NAND 플래시 관련 시스템 프로그래밍 특허가 승인되는데 기여했습니다.

60명 이상의 다른 공헌자들은, 모두 합치면 60년이 넘는 전문 기술 및 경력을 다음과 같은 회사 및 분야에서 가지고 있습니다.

애플, 바이두, Tencent, 아마존, 그리고 금융권에서는 암호학, 보안, 분산 시스템, 컴퓨터 네트워크, 시스템 개발, 시스템 설계, 인공지능, 데이터 채굴, 딥 러닝, 머신 러닝, 내장형 OS, 스토리지

, 네트워크 트래픽, 인공지능 모델 보안 개발, 시스템 보안, 그리고 분산 구조 안전성에서는 ACM 알고리즘, golang, C++

5. BlackPearl.Chain 시스템 설계 목표 및 핵심 솔루션

5.1 설계 목표

BlackPearl.Chain 팀은 대규모 상업 애플리케이션을 실행시킬 수 있는 차세대 퍼블릭 체인을 설계하고 개발했습니다. 목표는 다음과 같습니다.

● 완전한 탈중앙화, 선 팽창, 수 천만 TPS 를 노드의 증가와 동시에 지원, 몇 초 이내 거래 확정, 높은 안전성, 양자 컴퓨팅 및 바이오 컴퓨팅 공격에 저항성 존재, 전력 자원 미낭비, 초 저렴한 수수료(gas fee), 완전한 튜링 스마트 컨트랙트 플랫폼.

● VRF 컨센서스와 독보적인 경제 인센티브 모델로 각 개인의 경제적 권리와 이득의 균형을 만들어 내고, 게임 이론을 블록체인에 통합시켜 SHD 완전성을 창조

● 수십억 사용자 및 수 조(兆)개의 장비가 BlackPearl.Chain을 동시에 이용할 수 있도록 지원

5.2 핵심 솔루션

현재 이더리움 설계 구현에서, 모든 컨센서스 노드는 모든 거래 상태를 저장하는 완전한 블록체인을 저장합니다. 이는 이더리움의 안전성을 보장하지만, 또한 블록체인의 확장성을 제한합니다. 시스템의 프로세싱 파워가 증가하게 되면, 거대한 데이터 스토리지가 일반 사용자의 참여를 제한하게 될 것입니다.

시스템 확장성: BlackPearl.Chain은 샤딩 기술 솔루션을 이용하여 확장성 문제를 해결하고자 합니다. 노드의 수가 증가하면, 병렬 컴퓨팅의 컴퓨팅 성능이 증가하고, 시스템의 프로세싱 파워가 증가할 것입니다.

스토리지 솔루션: 데이터 분산 스토리지 기술은 높은 동시 실행 아래에 있는 블록 데이터 스토리지 문제를 해결하기 위해 채택되었습니다. 블록체인의 확장성 문제를 해결하기 위해 노드 수집, 분류 센터 슈퍼 스토리지 노드 및 스토리지 샤딩 기술을 추가하도록 설계되었습니다.

확장성과 스토리지 솔루션으로, 수천만 TPS가 실현될 수 있습니다.

6. 시스템 구조

6.1 시스템 단계

BlackPearl.Chain의 시스템 구조는 애플리케이션 단계, 컨트랙트(계약) 단계, 인센티브 단계, 컨센서스 단계, 네트워크 단계 및 스토리지 단계를 포함합니다.

애플리케이션 단계	WASM	DApp
스마트 계약 단계	Script	스마트 계약
인센티브 단계	온라인 파운데이션	스토리지 인센티브
	컬렉터 인센티브	어카운팅 인센티브
컨센서스(합의) 단계	Ethash 작업증명	Honey Badger 비잔틴 장애 허용 (BFT)
네트워크 단계	P2P 네트워크	네트워크 샤딩
	상태 샤딩	트랜잭션 샤딩
데이터 단계	샤드 서브체인 구조	수퍼 스토리지

	머클 패트리샤 트리 (MPT)	더블 어카운팅 데이터

그림 6.1: 시스템 구조

6.2 노드 구조

시스템 계약		WSAM	DApps
	인센티브	온라인 파운데이션	스토리지 인센티브
		컬렉터 인센티브	어카운팅 인센티브
	컨센서스(합의)	Ethash-작업증명	Honey Badger 비잔틴 장애 허용 (BFT)
암호화	gRPC		가십 프로토콜(Gossip)
RocksDB			
노드			

그림 6.2: 노드 구조

6.3 샤드 간 거래

그림 왼쪽부터

Collector node 컬렉터 노드

AI distribution center 인공지능 분산 센터

Shard A, B : 샤드 A,B

그림 6.3 : 샤드 간 거래

6.4 인센티브 모델

어카운팅 노드 인센티브	컬렉터 노드 인센티브	인공지능 분산 센터 인센티브	슈퍼 스토리지 노드 인센티브	온라인 사용자 기초 인센티브
거래 수수료 수집	거래 수수료(gas fee)를 기반으로 한 인센티브	거래 건수를 기반으로 한 인센티브	스토리지 용량을 기반으로 한 인센티브	거래 수수료 퍼센티지를 기반으로 한 로또

그림 6.4: 인센티브 메커니즘

6.5 시스템 구성 요소

그림 왼쪽부터

Tx 트랜잭션

Node 노드

Broadcast 전파

Leader 리더

Collector node 컬렉터 노드

Inter-shard communication 인터샤드 커뮤니케이션

Honey Badger 비잔틴 장애 허용(BFT)

Shard node 샤드 노드

Block 블록

Save all block 모든 블록 저장

Super storage node 슈퍼 스토리지 노드

Pull from groups 그룹에서 사용

Group 1,2,3 그룹 1,2,3

Distribution center 분산 센터

그림 6.5 시스템 구성 요소

그림 6.5에서 보다시피, 시스템 내에는 4가지 다른 타입의 노드가 있습니다.

●컬렉터

컬렉션 노드는 거래 정보를 수집하고 이를 해당 샤드의 특정한 어카운팅 노드에 전달하는 역할을 합니다. 컬렉션 노드는 거래를 응집함으로써 네트워크 커뮤니케이션의 수를 줄일 수 있으며, 네트워크 효율성을 향상시킬 수 있습니다.

●샤딩 노드

다른 서브 샤드들은 병렬적으로 채굴되며, 각 샤드들은 컨센서스에 내부적으로 도달합니다. 각 샤드는 각 샤드 안의 노드 스토리지 부하를 감소시키기 위해 스토리지 동시에 블록체인 데이터의 부분을 저장합니다.

●분산 센터

샤드 간 거래는 인터 샤드 커뮤니케이션을 필요로 하며, 분산 센터는 인터 샤드 커뮤니케이션을 해결하기 위해 도입되었습니다. 분산 센터는 거래의 수신자 따라 거래의 그룹을 형성하고, 수신 샤드는 리스펙팅 그룹에서 활발히 데이터를 수신합니다.

●슈퍼 스토리지 노드

샤드들의 각 노드가 원장 데이터의 부분만을 저장하기 때문에, 가끔씩 노드의 일부가 샤드 데이터를 얻거나 혹은 온샤드 컨트랙트를 문의하기 위해 오프라인이 될 수 있으며, 슈퍼 스토리지 노드는 모든 블록체인 데이터를 저장하기 위해 도입되었습니다.

7. 거래 프로세스

사용자에 의해 제출된 거래는 거래 풀에 수집되며, VRF 컨센서스에 의해 증명되고, 일괄 처리되며, 내보내 집니다. P2P 동기화는 거래가 확정되기 이전에 완료됩니다.

모든 거래 프로세스는 7단계로 나뉘어 있습니다. 거래가 처리되기 전에, 시스템은 네트워크 내 다양한 타입의 노드가 컨센서스를 통해 선출된 것인지 확실히 해야합니다. 거래 프로세스 단계는 그림 7-1에서 볼 수 있습니다.

1. 첫 번째로, 시스템은 컬렉션 노드, 샤딩 노드, 분류 센터, 컨센서스(합의) 알고리즘을 통해 네트워크 내에 요구되는 슈퍼 스토리지 노드를 생성합니다.

2. 클라이언트 A는 거래를 시작합니다. 예를 들어, 1 유닛의 화폐를 A라는 주소에서 B라는 주소로 전송하기 시작합니다. 전송을 시작하는 클라이언트 A는 거래를 개설해야 하고, 거래에 서명해야 합니다.

3. 클라이언트 A에 의해 시작된 거래와 다른 클라이언트에 의해 시작된 거래는 거래를 발송하기 위한 가장 가까운 컬렉션 노드를 선택하기 위해 라우팅 메커니즘을 사용합니다. 그 다음, 컬렉션 노드가 다수의 클라이언트에게서 다수의 거래를 수신하게 됩니다. 이는 거래를 해시(hash) 하고 각 거래의 목표 샤드를 찾아내며, 같은 목적지를 가진 샤드는 한 패키지에 같이 집합됩니다. 컬렉션 노드는 거래 팩들을 이웃한 컬렉션 노드에게 전파를 통해 보내고, 컬렉션 노드 리더는 거래 팩을 해당하는 타켓 샤드에 전달합니다. 컬렉션 노드 리더는 타깃 샤드를 향한 경로를 유지하는 역할을 하며 컬렉션 노드 리더는 순차 순환 대기 방식에 따라 회전하게 될 것입니다.

4. 클라이언트 A에 의해 시작된 거래가 주소 A에 따라 샤드 J로 해시(hash) 된다고 가정해 보겠습니다. 샤드 J가 컬렉션 노드 리더에 의해 전달된 거래 패키지를 받은 후, 거래 패키지 안의

거래들은 분해될 것이며 샤드 노드의 확인되지 않은 거래 풀에 추가될 것입니다. 그리고 거래는 샤드 내에서 넓게 전파될 것입니다. 샤드 노드는 가스에 따라 내림차순으로 거래 우선 순위를 매기고, 패키지 안에 있는 미확인된 거래 풀 내에서 거래를 선택할 것입니다. 샤드 노드는 첫 번째로 주소 A의 잔고를 1 유닛 코인으로 감소시키고, 그 후에 주소 B의 잔고를1 유닛 코인으로 증가시켜 달라는 요청을 분산 센터에 전송할 것입니다.

5. 슬라이스 J 내의 샤드 노드 리더에 의해 전송된 주소 B의 잔고 증가 작업 요청을 받고 나서, 분산 센터는 이 요청을 주소 B에 추가하고, 샤드 K의 해당하는 거래 프로세싱 대기열에 컬렉팅 노드와 같은 해시 알고리즘에 따라 추가합니다. 또한, 분산 센터는 샤드 J와 다른 샤드들, 이 샤드들의 해당하는 거래 프로세싱 대기열에 요청을 추가하여 각 샤드 노드 리더가 해당하는 대기열에서 메시지를 끌어오는 것을 기다립니다.

6. 샤드 K에서, 샤드 노드 리더는 처리 대기열에서 거래 패키지를 추출하기 위해 분산 센터에서 정기적으로 분산 센터에서 추출되고, 거래 패키지를 샤드의 다른 노드에게 전파합니다. 샤드 노드가 주소 B를 통화 1유닛 증가시키라는 작업 요청을 받으면, 주소 B의 잔고는 통화 1유닛만큼 증가되고, 주소 B에 의해 주소 A의 1 유닛을 받으려는 거래는 처리된 거래 풀에 추가됩니다. 그리고 샤드 노드는 샤드의 컨센서스(합의) 알고리즘에 따라 블록 거래 풀을 정산하고 생산하는 작업을 수행합니다. 샤드 K의 샤드 노드 리더는 주소 B의 잔고를 1유닛코인 증가시켰다는 작업 완료 요청을 분산 센터에 전송합니다.

7. 분산 센터가 샤드 J노드 리더에게서 주소 B의 잔고 1유닛 증가 완료 처리에 대한 요청을 받은 후, 분산 센터는 주소 A와 일치하는 샤드 J의 미결 상태인 처리 대기열에 요청을 추가합니다.

8. 샤드 J에서, 샤드 노드 리더는 분산 센터의 샤드 J 에 해당하는 거래 처리 대기열에서 거래 패키지를 정기적으로 가져오고, 거래 패키지를 샤드 J 내의 다른 노드에게 전파합니다. 특정한 샤드 노드가 주소 B를 1 유닛 증가하라는 요청의 완료를 처리했을 때, 대체 거래가 처리된 거래 풀에 추가됩니다. 마지막으로, 샤드 노드는 샤드의 컨센서스(합의) 알고리즘을 사용하여 새로운 블록 정산과 생산을 수행합니다.

Sender A 전송자 A

Collector node 컬렉터 노드

Shard J 샤드 J

Distribution center 분산 센터

Shard K 샤드 K

Send transaction 거래 전송

Leader sends trans pkg 리더가 거래 패키지 전송

Record 기록

Honey badger BFT consensus	허니 뱃저 비잔틴 장애 허용 컨센서스	Broadcast inter-shard trans pkg	인터샤드 거래 패키지 전파
Deduct balance from A	A에서 잔고 차감	Leader Pull inter-shard J trans pkg(include A->B finish)	리더 풀 인터샤드 J 거래 패키지 (A->B 완료 포함)
Leader pull shard K trans pkg (include B<-A confirm)	리더 풀 샤드 K 거래 패키지 (B<-A 확인 포함)	Broadcast trans pkg	거래 패키지 전파
Leader sends inter-shard trans pkg (include B<-A finish)	리더가 인터샤드 거래 패키지 전송 (B<-A 완료 포함)	Increase balance for B	B 잔고 증가시킴
Taken apart trans pkg	거래 패키지 분해	Broadcast transaction	거래 전파

Leader sends inter-shard trans pkg(include A->B finish)	리더가 인터샤드 거래 패키지 (A->B 완료 포함) 전송		

그림 7.1 거래 프로세스

8. 샤딩

확장성 솔루션으로서의 블록체인 샤딩은 2017년 후반 이후 많은 주목을 끌었습니다. 샤딩 기술과 함께, 많은 노드가 증가했고, 병렬 컴퓨팅의 연산력도 증가하였으며, 시스템의 처리 동력도 증가했습니다.

샤딩 메커니즘과 함께, BlackPearl.Chain은 거래 효율성을 향상시켰으며, 컴퓨팅 파워를 감소시키고, 스토리지 압력 또한 감소시켰습니다. BlackPearl.Chain 샤딩은 주로 네트워크 샤딩, 상태 샤딩, 스토리지 샤딩을 포함합니다.

8.1 네트워크 샤딩

네트워크 샤딩 메커니즘은 거래 풀 동기화, 컨센서스 및 샤드 내 블록 생산을 완성하며, 병렬 컴퓨팅은 다수의 샤드에서 수행됩니다. 병렬 컴퓨팅의 작업 수행은 참여 노드의 수와 함께 증가합니다.

네트워크 샤딩은 전체 채굴 네트워크를 4가지 종류의 노드로 나눕니다. 이는 위에서 설명되었 듯이 컬렉터 노드, 샤드 노드, 분산 센터와 슈퍼 스토리지 노드입니다.

슈퍼 스토리지 노드

슈퍼 스토리지 노드는 각 채굴 노드의 배열에서 수동적으로 유지됩니다. 원칙적으로, 모든 마이너 노드는 슈퍼 스토리지 노드에 글로벌 블록 원장을 얻기 위해 접근할 수 있습니다.

분산 센터 노드 선출

채굴자의 네트워크는 분산 센터 노드들을 선출하기 위해 Ethash-작업증명(PoW) 사용합니다. Ethash-작업증명(PoW) 연산을 완료한 노드들은 내림차순으로 순위 매겨집니다. 첫 번째 2nh 노드들은 후보 노드 풀에 선출되고, 후보 노드 풀의 노드들은 대역폭, 가능한 메모리, CPU, 디스크 스피드에 따라 내림차순으로 분류됩니다. 첫 번째 nh 노드들은 분산 센터 노드로서 선택됩니다. 또한 분산 센터 노드는 nh/20당 샤드의 수를 결정하여, 메시지가 분산 노드 메모리 내의 샤드에 의해 처리되도록 유지합니다.

분산 센터 노드 선출이 완료된 후, 채굴 네트워크는 Ethash-작업증명(PoW)을 통해 샤드 노드를 선출하고 이를 증명하기 위해 분산 센터에 제출합니다. Ethash-작업증명(PoW) 연선을 이때 완료한 노드는 내림차순 순서로 순위 매겨집니다. 첫 nh*ns/2- 노드들은 샤드 노드로써 선택되고, 모든 ns 샤드 노드는 1 샤드입니다.

컬렉션 노드 선출

채굴 네트워크는 컬렉터 노드를 Ethash-작업증명(PoW)을 통해 선출하고 이를 증명을 위해 분산 센터에 제출합니다. Ethash-작업증명(PoW) 연산을 이때 마친 노드들은 내림차순으로 순위가 매겨집니다. 첫 10*nco 노드들은 컬렉션 노드로서 선택되고, 10 컬렉션 노드씩 묶여집니다. 컬렉션 노드는 거래를 패키징하는데 사용되고, 이 패키지를 해당하는 목적지의 샤드에게 보내는 데 사용됩니다.

8.2 상태 샤딩

상태 샤딩은 각 주소에 해당하는 잔고와 스마트 컨트랙트 상태 정보를 해당하는 샤드로 나눕니다. 예를 들어, 주소 A의 상태 정보는 샤드 1에 유지되고, 주소 B의 상태 정보는 샤드 2에 유지됩니다. 주소 A가 주소 B에게 거래를 전송하기 시작하면, 샤드1의 주소A 잔고는 감소하고 샤드 2의 주소 B 잔고는 증가합니다. 샤드들 간의 커뮤니케이션은 분산 센터 내 To-be processed 메시지 대기열에 의해 수행됩니다. 또한 샤드는 to-be processed 메시지 대기열을 분산 센터에서 가져오고, 작업이 완료되면 분산 센터에 완료 요청을 보냅니다.

각 샤드는 분리된 체인을 생산하며, 그림 8-1에서 확인할 수 있듯이 샤드의 체인에는 거래 해시만이 기록됩니다. 완전한 거래 정보에 접근하려면, 슈퍼 스토리지 노드를 방문해야 합니다. 전체 채굴 네트워크는 샤드들의 수와 같은 숫자의 서브 체인을 생성할 것입니다.

Shard 0, 1, m 샤드 0,1,m

Root 루트

Block 0,L,U,V,T 블록 0,L,U,V,T

그림 8.1 각 샤드의 서브체인

8.3 스토리지 샤딩

각 샤드는 샤드 내의 거래 데이터만 저장합니다. 이 방식으로, 분산 스토리지 설계를 통해 스토리지 압력을 감소시킵니다.

9. 컨센서스(합의) 알고리즘

9.1 설계상의 가정

9.1.1 네트워크 내의 정상 노드(honest node)의 수는 언제나 우세하다.

9.1.2 노드들은 지원하지 않고서도 언제나 네트워크에 합류할 수 있다.

a.) BlackPearlChain 네트워크에서, 각 노드는 퍼블릭 키 주소로 나타납니다. (또한 월렛 주소) 새로 추가된 노드 주소의 경우, 네트워크의 다른 노드가 새로 결합한 노드로 성공적으로 전송된 후에 네트워크에서 합의를 도출하는 블록에 참여할 수 있습니다. (즉, 월렛 잔고는 n=100보다 커야함.)

b.) 악의적인 등록을 막기 위해, 각 참여자에게 대기 시간이 필요하며 컨센서스(합의) 프로세스에 참여하기 이전에 작업증명(PoW) 작업량 증명을 완료해야 합니다.

c.) 작업증명 작업량은 컴퓨팅 파워, 대역폭, 내부 및 외부 스토리지 속도 및 수용성을 포함한 성능 테스트를 포함합니다.

9.1.3 공격자는 또한 역학적으로 바뀔 수 있습니다. (정상 노드 역시 언제나 공격자로 바뀔 수 있습니다.)

9.2 BlackPearl.Chain 컨센서스(합의)

BlackPearl.Chain은 VRF(무작위 검증 기능) 컨센서스를 채택하고 업그레이드 합니다. VRF 컨센서스의 도입은 선출 과정을 예측 불가능하고 조종 불가능하게 합니다. 선택된 노드들은 샤드 컨센서스와 블록 생산 작업을 완료하고, 모든 블록체인 노드의 완전한 참여를 필요로 하지 않습니다. 작업은 샤드의 멤버 수가 증가하는 만큼 줄어들지 않습니다.

컨센서스 솔루션은 블록 생산 효율성을 향상시키고, 처리량을 향상시키며, 컴퓨팅 파워가 증명, 비교 및 블록 생산과 같은 작업에 효율적으로 집중할 수 있도록 합니다. 이 솔루션은 PoW(작업증명) 컨센서스와 관련된 사회적 자원의 낭비를 감소시킵니다.

BlackPearl.Chain VRF lightning fast(번개 속도) 컨센서스는 완전히 새로운 컨센서스 프로토콜로 빠른 상태 수집, 연산과 컨센서스 도달이 가능합니다. 이 메커니즘은 기존의 VRF와는 근본적으로 다른 것입니다.

기존의 VRF는 위원회를 형성하기 위해 제비 뽑기 식의 무작위 기능을 사용했으며, 합의는 위원회 멤버 간의 커뮤니케이션에 의해 결정되었습니다. 이는 커뮤니케이션 논쟁, 분리 및 뇌물 수수로 인한 효율성 감소에 취약하고 공정함에 쉽게 영향을 미치는 것입니다. BlackPearl.Chain은 중계 방송, 다수 사인(multi-signing), 상태 스위치 기술을 활용합니다. 우리의 독점적이고 독보적인 알고리즘과 프로세스로, BlackPearl.Chain은 기존 VRF 문제를 해결합니다.

각 샤드의 컨센서스 알고리즘은 허니 뱃져 비잔틴 장애 허용(Honey Badger BFT) 컨센서스를 사용하여 비동기 네트워크의 네트워크 상태를 더 잘 따라잡을 수 있으며, 오버헤드 커뮤니케이션을 감소시킬 수 있습니다. 컨센서스 알고리즘 수행 처리는 11단계로 나뉩니다.

1. 샤드 리더는 N 노드가 존재하는 현 에포크(epoch)를 시작하고, 샤드의 각 노드는 무작위로 거래 대기열에서 B/N 거래를 선택하며, (B는 전체 배치(batch) 사이즈입니다.) 임계값 암호화 알고리즘으로 암호화를 진행하기 위해 퍼블릭 키를 사용합니다.

2. 각 노드는 자체 암호화 거래 패키지를 다른 노드에 전파하고, BVAL 메시지를 거래 패키지에 투표하기 위해 전파합니다.

3. 노드가 다른 노드로부터 BVAL 메시지를 받는다면, 이 노드는 즉각적으로 반응하여 BVAL 메시지에 투표합니다.

4. 노드가 투표 혹은 거부 메시지를 수행하는 f+1 노드로부터 BVAL메시지를 받는다면, 또한 받은 투표 내용이 노드가 이전에 보낸 내용과 다르다면, f+1노드들과 같은 투표 메시지가 보내집니다.

5. 노드가 2f+1 기타 노드들에 의해 전송된 투표 혹은 투표 거부 메시지를 받는다면, 이 노드는 받은 메시지와 같은 투표 내용의 AUX 메시지를 전파합니다.

6. 노드가 N-f 기타 노드에 의해 발송된 투표 메시지를 받는다면, 이 노드는 다른 노드들에게 투표 거부를 전송합니다.

7. 노드는 네트워크가 N-f AUX 응답 메시지에 응답하는 것을 기다리며, Vals 가치를 AUX 응답 메시지 내 주요 투표로 설정합니다.

8. 노드는 AUX메시지의 주요 투표가 BVAL메시지의 주요 투표와 일치한다면, 그리고 결과가 코인 가치 S와 같다면 이 에포크(epoch)의 코인 가치 S를 얻습니다. 그러고 나서, 노드의 전파되고 암호화된 거래 패키지가 ACS(Asynchronous Common subset)에 참여할 것입니다.

9. 각 노드는 ACS 내 각 거래의 임계값 협약 암호 해독을 수행하고, 암호 해독 결과를 다른 노드들에게 전파합니다.

10. 노드는 f+1 암호 해독 결과를 받기 위해 기다리고, 임계값 암호 해독 알고리즘과 퍼블릭 키를 사용하여 받은 암호화 결과를 해독합니다. 마지막 결과는 원래의 거래가 될 것입니다. 또한 원래 거래는 가벼워지고 정리될 것이며, 이는 기록되는 마지막 거래가 될 것입니다.

11. 샤드 리더는 위의 단계를 거친 거래를 포함한 블록을 생산할 것이며, 현 샤드의 서브체인에 이를 기록할 것입니다.

Node i, j k : 노드 i, j, k

Random select B/N transaction 무작위 선택 B/N 거래

Vi=TPKE.enc(Pk, txs)

RBCi multicast Vi

Bai multicast BVAL(Vi,1)

RBCj multicast Vj

Bai multicast BVAL(Vj,1)

Waiting for f+1 Bai BVAL(Vi,b)

If b=-, then Bai multicast BVAL(Vi,0)

If received N-f value 1 from BA(I,j, …) (without K) BAk multicast BVAL(Vk,0)

Waiting for 2f+1 Bai BVAL(Vi,b)

Bai multicast AUX(Vi,b)

Waiting for N-f BAiAUX(Vi,b)

Vals, most often b

S=Coin, GetCoin()

If vals = b = S, then Bai=B

Else looping

BA agreement on ACS[r]

Decrypt each transaction package within ACS[r], ej=TPKE.DecShare(Ski,Vj)

- ACS[r], ej=TPKE.DecShare(Ski,Vj)내의 각 트랜잭션 패키지를 해독함

RBCi multicast DEC(r,j,I,ej)

RBCi multicast DEC(r,j,I,ej)

Waiting for f+1 DEC (r,j,I,ej)

Decrypt, and get transaction tx=TPKE.Dec[PK, [PK, ((k,ek)…)]

Ordering the transaction and reproduce the block

- 거래 정리 및 블록 재생성

그림 9.1 허니 뱃처 비잔틴 장애 허용 (BFT) 컨센서스

10. 스토리지 시스템

10.1 블록 구조

각 블록은 다수의 거래로 구성됩니다. 거래가 포함하는 필드를 먼저 살펴 보겠습니다. 거래 어카운트는 비트코인의 UTXO(미지출 거래 출력) 대신 이더리움의 계좌 시스템을 사용합니다. A가 B에게 돈을 송금합니다. 가장 기본 필드는 A의 계좌 번호, B의 계좌번호와 송금하는 돈의 금액입니다. 비트코인은 UTXO를 이용해서 이중 지출 문제를 해결하고, 각 미지출 출력은 한 번만 참조될 수 있습니다. 이더리움 어카운트 시스템과 비슷하게, 이중 지출과 반복되는 공격을 해결하기 위해 논스(nonce) 필드가 도입됩니다. 각 어카운트는 하나의 논스 필드를 가집니다. 각 거래가 전송되면, 논스는 자동적으로 1만큼 증가됩니다.

이더리움처럼, BlackPearl.Chain은 가스(gas)를 도입합니다. 시장에서 토큰의 가격은 끊임없이 변동하고, 스마트 컨트랙트 실행을 위해 필요한 컴퓨팅 자원은 상대적으로 고정되어 있습니다. 따라서 컴퓨팅 자원을 측정하기 위해 가스가 도입됩니다. 가스가 도입된 후, 무한 루프로 스마트 계약을 실행하는 해커들의 공격을 방어하기 위해 gas_limit(수수료 상한선)을 추가해야 합니다. 또한, 스마트 컨트랙트의 처리 시간을 낮은 수준으로 유지하여 시스템의 거래 효율성을 향상시켜야 합니다.

요약하자면, 한 거래는 다음과 같은 필드를 포함합니다.

누구에게서(from): 거래 전송자 주소

누구에게로(to): 거래 수신자 주소

가치(value): 전송된 디지털 화폐 수

논스(nonce): 다른 거래들의 같은 사용자임을 구분하는 표시

가스 가격(Gas_price): 전송자가 지불하고자 하는 가스의 가격

가스 리밋(gas_limit): 거래를 실행함으로써 소비될 수 있는 가스의 최대 양

거래가 생성되고 나서, 거래는 서명이 필요하며, 먼저 해시 과정을 거친 후 프라이빗 키로 암호화 될 것입니다.

Header 헤더		
ParentHash	txRoot 트랜잭션 루트	StateRoot 상태 루트
gasLimit 가스 리밋		
gasUsed 사용된 가스		

Merkle Patricia tree 머클 패트리샤 트리

Root 루트

Tx 거래(트랜잭션)

From 발신자		Nonce논스
To수신자		Balance 잔고
Nonce 논스		Storage root 스토리지 루트
Gas price 가스 가격		
Gas limit 가스 리밋		

그림 10.1 블록 스토리지 구조

비트코인은 머클 트리를 거래 스토리지에 사용합니다. 머클 트리를 사용하는 것의 장점은 루트 해시들을 비교함으로써 전체 블록의 통합을 증명하기가 쉽다는 것입니다. 블록이 변조되었는지 입증할 필요가 있을 때, 현 블록을 노드의 작은 부분의 해시를 계산하는 루트 노드로 확장하기만 하면 됩니다. 새로운 노드를 추가할 때는 모든 블록의 해시를 다시 계산할 필요가 없고, 일부 노드의 해시만 다시 계산하면 됩니다.

10.2 상태 구조

계좌 시스템을 추가한 후, 각 사용자 상태는 다음의 데이터를 포함합니다.

Nonce 논스: 현 주소에서 전송된 거래의 수

Balance 잔고: 현 주소가 소유한 잔고

StorageRoot 스토리지 루트: 계약 데이터

거래 데이터 내역과는 다르게, 사용자의 상태 데이터는 자주 업데이트 될 필요가 있습니다. 매번 거래가 시작될 때마다, 계좌의 논스와 잔고는 업데이트 되어야 합니다. 또한, 네트워크에 끊임없이 새로운 사용자가 추가됩니다. 특정 유저의 잔고 문의를 쉽게 하기 위해서, 효과적인 데이터 구조는 계좌 데이터의 빠른 검색, 추가 및 수정이 필요합니다. 또한 데이터의 확인이 용이하고, 데이터가 변조되는 것을 방지하는 것이 필요합니다. 이더리움은 향상된 머클 패트리샤 트리를 제안했으며, BlackPearl.Chain 퍼블릭 체인 역시 상태 데이터와 거래 데이터를 저장하기 위해 머클 패트리샤 트리를 이용할 것입니다.

구체적인 구조는 다음과 같습니다.

[그림]

<table>
<tr><td colspan="3">Block Header 블록 헤더</td><td colspan="3">Block Header블록 헤더</td></tr>
<tr><td>PrevBlockHash
이전 블록 해시</td><td>Nonce 논스</td><td></td><td>PrevBlockHash
이전 블록 해시</td><td>Nonce 논스</td><td></td></tr>
</table>

StateRoot 상태 루트	TxRoot 트랜잭션 루트	ReceiptsRoot 영수증 루트	StateRoot 상태 루트	TxRoot 트랜잭션 루트	ReceiptsRoot 영수증 루트

Branch Node		Branch Node	
Key-prefix	Hash해시	Key-prefix	Hash 해시
ab		ab	

Key-prefix

Hash 해시

Leaf node 단말 노드		Leaf node 단말 노드		Leaf node 단말 노드		Leaf node 단말 노드	
Key-prefix	Hash 해시	Key-prefix	Hash 해시	Key-prefix	Hash 해시	Key-prefix	Hash 해시
123	10	456	20	789	100	789	110

그림 10.2 머클 패트리샤 트리 구조

10.3 스토리지 샤딩 기술

BlackPearl.Chain 퍼블릭 체인은 전체 시스템의 처리량을 병렬 컨센서스, 블록 생산, 스토리지를 통해 향상시키기 위해 샤딩 기술을 사용합니다.

샤드의 스토리지 전략은 다음과 같이 설계됩니다.

이중 지출 문제를 방지하기 위해, 필드를 기반으로 각 거래는 특정 샤드로 해시될 것입니다. 각 특정 샤드 노드는 일부 사용자의 상태와 거래만을 저장합니다.

병렬 컴퓨팅으로 체인의 데이터가 급격히 증가함에 따라, 샤드의 각 노드는 모든 사용자의 상태와 거래를 저장해야 하고, 이는 스토리지에 큰 부담을 주어 일반 노드의 한계치 접근을 증가시킬 것입니다. 따라서, 슈퍼 스토리지 노드만이 모든 사용자의 상태와 거래 데이터의 완전한 양을 저장할 것입니다.

10.4 슈퍼 스토리지 노드

슈퍼 스토리지 노드는 거래와 사용자 정보를 모든 샤드에 저장해야 합니다. 스토리지 노드가 실패한 후 데이터 손실을 방지하기 위해, 슈퍼 스토리지 노드는 클러스터 배포 메커니즘(cluster deployment mechanism)을 채택합니다.

[그림]

Slave 슬레이브

Master distribution node 마스터 분포 노드

Zookeeper cluster 주키퍼 클러스터

LevelDB

그림 10.3 슈퍼 스토리지 노드

마스터 분포 노드는 요청을 일정시키고 특정 leveldb 노드에 특정한 요청을 분배하는 역할을 합니다. 마스터 분포 노드는 백업(backup)이 있습니다. 마스터 분포 노드가 실패할 경우, 슬레이브 분포 노드가 요청을 대신 맡게 됩니다.

각 leveldb 소형 클러스터는 한 샤드에 해당하는 데이터를 저장합니다. Leveldb 클러스터의 메인 노드를 선택하기 위해 주키퍼(Zookeeper)를 사용합니다. Leveldb 클러스터 내의 복제 노드 역시 존재합니다. 복제 노드는 메인 노드와 데이터를 계속 동기화하기 위해 commit log를 사용합니다.

Leveldb 내의 매인 노드가 실패할 경우, 주키퍼는 메인 노드만큼 데이터를 업데이트하여 소유하고 있는 복제 노드를 선택합니다.

주키퍼 클러스터 노드는 분산 일관성 알고리즘(distributed-consistent algorithm)을 통해 함수 정보의 일관성을 보장합니다. 글로벌 원장(global ledger)의 신뢰성은 그림 10.3에 나와있는 것처럼 슈퍼 스토리지 노드의 고가용성 구조에 의해 보장됩니다.

11. 인센티브 모델

샤딩 구조 설계는 병렬 노드 증가 만큼의 시스템 처리 동력의 증가를 보장합니다. 퍼블릭 체인은 노드가 활동 중인 온라인 거래 노드를 통해 시스템에서 온라인 거래 시간과 더 많은 참여를 증가시키도록 조장합니다. 각 샤드의 어카운팅 노드는 수수료가 청구될 때 0.01%의 수수료를 퍼블릭 체인 파운데이션 주소에서 받으며, 계좌 내의 금액은 온라인 거래 노드의 무작위 보상으로 사용됩니다.

거래와 스마트 컨트랙트의 실행은 수수료(gas fee)의 적용을 받고, 사용자는 가스의 가치와 각 거래의 최대 가치를 설정할 수 있습니다. 거래 처리의 단계마다 해당되는 역할들은 특정한 양의 수수료(gas fee)를 얻습니다. 이 분산 센터 노드의 총 수입과 슈퍼 스토리지 노드는 자동적으로 블록체인에 의해 생성되며, 각 샤드의 어카운팅 노드에 의해 컨센서스가 기록된 후에 효과를 발휘합니다.

11.1 어카운팅 노드 보상(reward)

어카운팅 노드가 블록을 생산할 때, 거래 처리 수수료(gas fee)가 어카운팅 노드에 의해 수집됩니다. 일반적으로, 하나의 거래 전송 수수료(수집 노드 보상분을 제외한 후의 금액)는 발신자와 수신자 모두에게 공평하게 분배됩니다. 만약 거래 수행에 실패하면, 수수료는 어카운팅 노드에 의해 완전히 청구될 것입니다. 스마트 컨트랙트를 실행할 시에, 만약 거래 실행이 실패했을 경우 혹은 설정된 시간 내에 반환에 실패했을 경우, 어카운팅 노드는 남은 수수료를 수집합니다. 각 어카운팅 노드는 가스를 충전할 때, 0.01%를 퍼블릭 체인 파운데이션 주소에서 가져옵니다.

11.2 컬렉션 노드 보상

컬렉션 노드는 거래를 수집하고 패키징하며, 이를 각 샤드의 어카운팅 노드에 전송하고, 수수료(gas fee)를 얻습니다. 수수료 보상 비율은 고정되어 있습니다. 컬렉션 노드가 거래 데이터를 통합할 때, 컬렉션 노드는 자신의 수입을 수수료에 기반하여 계산하고, 자체 증가를 위해 거래 기록을 추가합니다. 샤드의 어카운팅 노드는 컬렉션 노드에 의해 보내진 거래 데이터를 검증하고, 수수료 보상 계산이 정확한지를 확인하며, 컨센서스로 승인하며 기록을 위해 블록에 내용을 기재합니다.

11.3 분산 센터 노드 보상

분산 센터는 처리될 거래(To-be processed transaction)의 양에 따라 보상을 얻습니다. 컬렉션 노드에 의해 전송된 거래가 승인되면, 샤드 노드는 거래를 거래 패키지에 추가하고, 이는 처리될 거래의 양과 퍼블릭 체인의 내장된 수치 정보에 따라 분산 센터 노드의 잔고를 증가시킬 것입니다. 그러고 나서, 이 거래 패키지는 분산 센터로 보내질 것입니다. 샤드에 의한 합의 이후에, 거래는 확정되고, 보상은 유효화 됩니다.

11.4 슈퍼 스토리지 노드 보상

슈퍼 스토리지 노드는 블록체인 데이터를 저장하고 거래와 계약 문의 서비스를 제공합니다. 슈퍼 스토리지 노드의 보상 총 수입은 제공된 서비스의 저장된 데이터의 양에 기반합니다. 각 샤드의 어카운팅 노드는 스토리지 노드 잔고 증가 거래를 슈퍼 스토리지 및 퍼블릭 체인에 내장된 수치 정보와 동기화된 데이터의 양(byte)에 따라 추가합니다. 합의 이후에, 거래는 확정되고, 보상은 유효화 됩니다.

11.5 사용자 온라인 파운데이션 무작위 보상

퍼블릭 체인은 사용자를 위한 무작위 보상을 사용하여 사용자가 블록체인 시스템을 거래와 스마트 컨트랙트 애플리케이션을 운영하는데 사용하도록 돕습니다. 특정한 알고리즘에 따라서, 각 거래 정보가 생성될 때, 거래 정보는 동시에 샘플화되고, 해시 가치는 계산됩니다. 어카운팅 노드가 거래를 확인할 때, 해시 가치와 샤드에 존재하는 거래 주소의 해시 가치를 비교합니다. 이 둘이 일치하면, 거래 개시자는 온라인 펀드 보상을 받습니다. 어카운팅 노드는 해당하는 거래 주소에 보상을 들이기 위해 스마트 거래 콜이 필요합니다. 스마트 거래가 퍼블릭 체인에 배치된 후 정해진 규칙에 따라 확인될 것이고, 요건을 충족하는 거래 개시자는 파운데이션 주소에서 거래 시작 주소로 보상 분배를 완료하기 위해 거래를 전송을 수행할 것입니다.

12. 신뢰할 수 있는 컴퓨팅에 의한 시스템 업그레이드

현재, 비트코인과 이더리움은 비트코인 확대에 따른 하드 포크와 ETA 해킹 사건으로 일어난 하드포크 등 개발 과정에서 일부 문제점들을 겪고 있습니다. 블록체인 업그레이드 시 발생되는 문제를 해결하고, BlackPearl.Chain은 역동적인 업그레이드를 달성하기 위해 신뢰할 수 있는 컴퓨팅을 사용하는 방법을 제안합니다.

12.1 인공지능 예측

시스템 업그레이드는 커뮤니티 멤버의 이득을 고려해야 하는 동시에 업그레이드가 커뮤니티에 끼칠 영향 또한 고려해야 하기 때문에 BlackPearl.Chain은 인공지능 시스템과 투표 조합을 사용합니다. 업그레이드 된 인공지능 시스템은 과거 업그레이드가 커뮤니티에 미치는 영향(사용자 규모, 커뮤니티 붐 등)을 이용하여 업그레이드가 필요한지 여부를 예측합니다. 업그레이드 내역 데이터가 더 풍부해지면, 업그레이드된 인공지능 시스템 역시 더 지능적이게 될 것입니다. 인공지능에게 모든 것을 맡기는 것은 불확실하기 때문에, 커뮤니티 투표와 인공지능을 결합합니다. 인공지능과 커뮤니티 투표는 업그레이드의 50%씩을 차지합니다.

12.2 이중 디렉토리 업그레이드

이중 디렉토리 업그레이드 방법은 프로그램을 업데이트 할 때 사용됩니다. 백그라운드 업데이트 동안 운영되는 모든 파일은 점유되며 업데이트 될 수 없습니다. 그러므로, 이전 버전이 다른

디렉토리에 복제되고 그 후에 새롭게 복제되는 프로그램 파일이 업데이트 됩니다. 동시에, md5 통합 체크가 새로운 버전에서 수행됩니다. 부트(boot) 과정은 부트로더(bootloader)를 운영하는 것과 같습니다. 부트로더의 논리는 버전 번호를 감지하고 최신 버전의 애플리케이션 처리를 불러오는 것입니다. 부트로더의 논리가 간단하기 때문에, 부트로더에 대해서는 업데이트가 거의 필요하지 않습니다.

13. 어카운트(계정) 시스템

13.1 어카운트 생성

어카운트 시스템은 이더리움 어카운트 시스템의 설계에 의존합니다.

어카운트에는 두 가지 종류가 있습니다. 사용자 어카운트와 계약 어카운트 입니다. 사용자 어카운트로는, 프라이빗 키를 통해 거래를 보낼 수 있고, 계약 코드를 발동할 수 있습니다. 계약 어카운트는 거래 혹은 다른 계약으로부터 수신한 메시지의 실행을 통해 발동된 관련 코드가 있습니다.

사용자 어카운트는 한 쌍의 퍼블릭 및 프라이빗 키로 정의됩니다. 한 어카운트의 특정한 생성 과정은 그림 13.1에 나와 있습니다.

Start	시작
Ecdsa produce public and private key	Ecdsa가 퍼블릭 및 프라이빗 키 생성
Take Keccak256(pubKey) last 20 bytes as address	Keccak256(퍼블릭키) 마지막 20바이트를 주소로 사용
User password to encrypt private key and save	프라이빗 키를 암호화 할 사용자 비밀번호 및 저장
End	끝

그림 13.1 어카운트 생성 과정

먼저, 프라이빗 과 퍼블릭 키는 타원 곡선 디지털 서명 알고리즘(secp256k1 곡선)에 의해 생성됩니다. 그러고 나서 Keccak256을 퍼블릭 키를 해시하기 위하여 사용하고 마지막 20바이트를 어카운트 주소로 사용합니다. 마지막으로, 프라이빗 키는 사용자에 의해 입력된 비밀번호로 암호화되고, 퍼블릭 키와 함께 키 저장 파일에 저장됩니다. 키 저장소는 비밀번호를 사용하여 암호화 된 프라이빗 키가 있는 Json 텍스트 파일에서 읽을 수 있습니다.

어카운트가 생성될 때, 어카운트 정보는 상태 루트에 바로 들어가지 않을 것입니다. 이는 해커가 대량의 새로운 어카운트를 만들어 냄으로써 시스템을 공격하는 것을 방지하기 위함입니다.

13.2 어카운트 수입 지원

유효한 키 저장소 파일을 구축하여 계정을 가져옵니다. 키 저장소 파일 내의 프라이빗 키는 암호화 되어있지 않으며 계정을 가져올 때, 프라이빗 키를 암호화하기 위하여 비밀번호를 입력해야 합니다 .

13.3 프라이빗 키 복구

프라이빗 키를 잃어버리는 것은 계정의 비밀번호를 잃어버린 것과 같으며 계정 내의 모든 코인들이 분실됩니다.

기존의 솔루션은 키 저장소와 비밀번호를 백업해 놓는 것이며 백업을 통해 계정의 퍼블릭 및 프라이빗 키를 완전히 복구할 것입니다.

다른 방식은 사용자의 프라이빗 키를 다수의 복제판으로 나누고, 나눠진 각 복제키를 각기 다른 머신에 저장해 놓는 것입니다. XOR 결과 또한 복제로 저장합니다. XOR 작업에 기반한 규칙은 다음과 같습니다.

예를 들어, d = a^b^c

이 때

a = d^b^c

b = d^a^c

c = d^a^b

머신 중 하나가 실패하면, 다른 여러개 머신들의 키들을 XOR 함으로써 복구가 가능합니다.

14. 스마트 컨트랙트

14.1 스마트 컨트랙트 플랫폼 및 호환성

고성능 블록체인 서비스를 제공하기 위해, BlackPearl.Chain은 병렬 실행 및 호환 가능한 스마트 컨트랙트 플랫폼을 설계했습니다. BlackPearl.Chain 가상 기계 설계는 스마트 컨트랙트 작업을 지원하고 이더리움이나 EOS와 같은 기존의 퍼블릭 블록체인 스마트 컨트랙트 애플리케이션의 호환 가능한 지원을 제공합니다.

EOS를 위해 WebAssembley(WASM)을 사용할 계획이 있으며, 이더리움 스마트 컨트랙트 역시 WASM에 사용될 것입니다. (https//github.com/ewasm/design)

이는 BlackPearl.Chain에 더 많은 스마트 컨트랙트 애플리케이션(DApp)들이 옮겨지도록 보장합니다

.

스마트 컨트랙트는 고성능 웹 애플리케이션을 구축하는 데 사용될 수 있으며 소량의 개조로도 샌드박스 또한 될 수 있습니다.

14.2 스마트 계약 플랫폼 유사점

스마트 계약이 실행될 때, 다음의 3가지 서브 프로세스가 확인 및 검증되어야 합니다.

a) 메시지 내부 일관성

b) 모든 전제 조건이 유효한지

c) 애플리케이션 상태 수정

처음 두 번째 단계는 읽기 전용이며 병렬로 실행될 수 있습니다. 마지막 단계는 애플리케이션을 수정하는 단계임으로 각 애플리케이션을 순서대로 처리해야 합니다.

샤딩의 장점은 스마트 컨트랙트의 병렬 실행 효율성을 향상시킨다는 것입니다. 샤딩 사용으로 인해, 스마트 컨트랙트의 스토리지와 실행 또한 해결책을 찾을 필요가 있습니다.

계약이 전개되면 데이터는 로컬 샤드에 먼저 기록되고 슈퍼 스토리지 노드에 동기화되어 전체 네트워크의 스마트 컨트랙트 데이터를 통합합니다.

BlackPearl.Chain은 다음의 문제를 해결해야 합니다.

다른 샤드들에서 어떻게 스마트 컨트랙트를 빠르게 얻고 실행할 수 있을까?

네트워크 전체에서, 슈퍼 스토리지 노드만이 스마트 컨트랙트의 완전한 전개를 이해합니다. 분산된 데이터 스토리지 때문에, 개개인의 샤드 노드가 다른 샤드에 저장된 계약 정보를 직접적으로 얻을 수 있는 방법은 없으며, 슈퍼 스토리지 노드에 의해 문의 서비스가 제공되어야 합니다.

슈퍼 스토리지 노드의 서비스 수용력, 노드의 개수와 전체 네트워크의 TPS를 고려하여, 설계는 각 샤드 노드와 슈퍼 스토리지 노드를 분리하고, 싱글 스토리지 노드의 수행 압력을 감소시킵니다.

14.3 프라이빗 키 복구

인터 샤드 스마트 컨트랙트 실행은 중첩된 호출로 이어질 수 있습니다. 스마트 컨트랙트 실행의 정확성을 어떻게 보장할 수 있을까요?

스마트 컨트랙트가 중첩 호출에 존재할 때, 모든 실행이 다수 샤드의 특정한 순서를 따라야 할 경우가 있을 것입니다.

계약 실행을 발동하는 어카운팅 샤드 노드는 시간 타임 슬라이스의 숫자 내에서 계약 실행을 완료해야 할 것이고, 수수료가 청구될 것입니다.

Smart contract 스마트 컨트랙트

Contract node 1 계약 노드 1

Distribution center 1,2,3 분산 센터 1,2,3

Node 노드

Wait b->c b->c 대기

Shard 1,2,3 샤드 1,2,3

그림 14.1 스마트 계약 인터샤드 실행

그러나, 계약 실행이 샤드를 가로질러 수행되기 때문에, 발동된 샤드가 결과를 기록하고 블록에 들어가기 이전에 다른 샤드가 코드를 실행하고 블록을 생산하기를 기다려야 할 필요가 있습니다. 데이터 기록에는 순서가 있습니다. 블록 생산은 계약 호출 프로세스와는 분리되어 있습니다. 마지막 계약 호출이 블록에 첫 번째로 기록됩니다. 분산 센터가 이를 업데이트 한 후, 이전 샤드가 작업을 기록하고 블록에 들어갈 수 있습니다.

또한, 같은 샤드에서, 어카운팅 노드는 블록의 기록 결과 이전에 거래와 계약 상태를 동기화하고 저장해야 합니다.

계약 실행이 실패할 경우, 데이터는 되돌려집니다. 수수료 수집과 각 샤드의 상태를 복구하는 데 집중해야 할 필요가 있습니다. 실행 프로세스는 그림 14.1에 나와있습니다.

15. 로드맵

2019/Q2

내부 테스팅 네트워크 배포: 핵심 모듈 업데이트, 월렛 사용자 인터페이스 업데이트, 거래 풀 최적화, 컨센서스 업데이트, 블록체인 익스플로어(Blockchain Explorer) 업데이트.

2019/Q3

퍼블릭 테스트를 위한 테스트넷 배포: 네트워크 샤딩, 거래 샤딩, 슈퍼 라우팅, 슈퍼 스토리지 노드, 스마트 계약 플랫폼 업데이트. 생태계 참여: 사용자, 개발자

2019/Q4

완전한 기능을 갖춘 테스트넷 배포: 상태 샤딩, 몇 초 내에 확정, 수백만 TPS, 시스템 계약, 양자 연산 저항

2020/Q1

메인넷 라이트 배포: 퍼블릭 체인 매핑(mapping), BNS 뉴론 통치 방식, DApp SDK, IPFS 스토리지, 선팽창

2020/Q2

메인넷 배포

2020/Q3 그리고 이후

BPL_결제 DApp, BPL_메시지 DApp, 메인넷 업데이트

16. 팀

Sarah (Ping) Li

CEO, 공동 창업자

기술 에반젤리스트(Evengelist)

前 애플, 샌디스크, 삼성, 소니 근무

Jack Liu

최고 기술 책임자(CTO), 공동 창업자

저명한 블록체인 과학자, 보안 광

연쇄 창업가, Tencent 수석 설계자, OkEx 수석 과학자

Kaustav Chaudhuri

고문단, 커뮤니티 설계자

Pitch 글로벌 네트워크 창업자, 저자, 연설가

Bill Kallman

고문단, 벤처 투자가

연쇄 창업가, Moby 창업자, GET 그룹 공동 창업자, Timberline 투자

17. 토큰 모델

토큰 심벌: BPLC

총 토큰 공급량: 64,000,000,000(일정한 공급, 규모 변경 없음)

Token distribution ratio 토큰 분배 비율

12% founding team 창업 팀

28% company incorporation and R&D 회사 법인 및 연구 개발

40% Developers & community 개발자 및 커뮤니티

20% token sale 토큰 세일

그림 16.1 토큰 모델

BPLC 토큰은 초기 ERC20 이더리움 표준에 기반하여 변동성이 감소된 구조적 유틸리티 토큰입니다. 메인넷이 준비되면, ERC20 토큰은 BlackPearl.Chain 본래의 토큰으로 변환될 것입니다. 처음에, 토큰은 프로젝트의 연구개발을 위한 주요 자원으로 사용될 것입니다. 이후에는 BlackPearl.Chain 플랫폼을 가동할 주요 도구로 사용될 예정입니다. BLPC토큰을 사용하는 데에 요구되는 몇 가지의 다른 기능들이 있습니다. DApp과 스마트 컨트랙트 실행, 노드로서의 사용자 참여 및 BlackPearl.Chain 플랫폼 생태계 참여자를 위한 인센티브 보상입니다.

토큰 세일 요약

이 백서는 토큰의 분배와 토큰 런칭 세부사항을 설명합니다. 또한 BlackPearl 토큰의 목적을 간단히 설명하고 BlackPearl 플랫폼 내 기능을 설명합니다.

BlackPearl Platform은 전 세계 사용량(70억 명)과 10T 장치를 동시에 실행할 수 있도록 하며, 수백만 TPS와 초 단위 지연을 가능하게 합니다.

BlackPearl은 기업 수준의 분산 애플리케이션을 가능하게 하는 확장 가능한 처리량을 가진 인프라입니다. BlackPearl 토큰은 애플리케이션이 스마트 컨트랙트 지시를 실행하기 위해 수수료를 지불하는 것을 가능하게 합니다. 토큰은 또한 BlackPearl 블록 생산자 노드, 슈퍼 스토리지 노드와

같은 네트워크 생태계 참여자들에게 자동적으로 보상을 주기 위해서 퍼블릭 체인 소프트웨어에 의해 사용됩니다.

토큰 사용

토큰 런칭의 경우, BlackPearl은 공공 기부를 위해 BPLC 토큰을 발행할 것입니다. 토큰은 의도된 기능에 따라 유틸리티 토큰으로 분류될 것입니다.

BlackPearl 발전을 위한 펀딩은 일련의 크라우드 세일을 통해 진행될 것입니다. BlackPearl 플랫폼의 초기 펀딩은 12,800,000,000개의 초기 토큰 중 800,000,000개의 토큰을 제공하는 크라우드 세일을 통해서 진행될 것입니다. 토큰은 두 크라우드 세일에 걸쳐 분배될 것입니다. 기간 1: (1) 프라이빗 프리세일, 이어서 (2) 퍼블릭 세일 (2019년 5월 23일부터 2019년 9월 22일까지 1BPLC당 0.075$). 두 번째 기간 크라우드 세일은 4,000,000,000개의 초기 토큰을 제공할 것입니다 (2019년 9월 23일부터 2019년 12월 22일까지, 1BPLC당 0.10$). 세 번째 기간 크라우드 세일은 8,000,000,000개의 초기 토큰을 제공할 것입니다 (2019년 12월 23일부터 2020년 6월 22일까지 1BPLC당 0.15$).

BPLC 토큰

BPLC토큰은 ERC20으로 구현된 이더리움 기반 토큰이며 참가자가 블록체인 생태계 구축에 기여하고 참여할 수 있는 유틸리티 토큰입니다.

12,800,000,000개의 토큰은 일련의 크라우드 세일 이후에 존재할 것이며 모든 토큰 세일 시리즈가 끝난 후에는 토큰은 더 이상 발행되지 않을 것입니다. 판매를 위한 12,800,000,000개의 토큰은 폭넓은 분배를 보장하기 위해 전체 토큰 공급의 20%를 차지합니다.

토큰 판매 세부사항

토큰 심볼	BPLC
프라이빗 프리 세일	프라이빗 프리세일은 퍼블릭 세일 이전에 진행됨

퍼블릭 세일, 기간1	2019년 6월 23일 - 2019년 9월 22
소프트 캡	미국달러 500,000$
하드 캡	미국달러 60,000,000$
사용 가능한 생성된 최대 토큰 개수	64,000,000,000 토큰
구매 가능한 최대 토큰 개수	800,000,000 토큰(기간1)
플랫폼(토큰 타입)	이더리움(ERC20)
통용 통화	이더리움, 비트코인, 법정화폐
ETH/USD BTC/USD 비율	ETH와 BTC 가격은 퍼블릭 세일 시작 하루전에 정해짐 토큰 론칭은 퍼블릭 세일이 종료되거나 하드 캡에 도달하면 완료됨
토큰 공개 일정	토큰은 퍼블릭 세일 날짜에 분배 시작될 예정
토큰 당 미국달러 가격, 기간1	미국달러 0.075$

위험 요소, 공개, 확인 및 구매자에 의한 보증 및 기타 안내문

중요 알림: 예비 구매자는 토큰 구매가 적절한 투자인지 여부를 결정하는 데 수반되는 위험을 주의 깊게 고려해야 하며, 그 중 일부는 아래에 요약되어 있습니다.

본 절에서는 문맥에 따라 달리 요구되지 않는 한, 아래에 제시된 위험 요소와 공시는 BlackPearl 토큰과 관련해 적용되는 것으로 간주되며, 토큰에 대한 참조 또한 BlackPearl 토큰에 대한 참조로 간주됩니다.

토큰과 관련된 공시

토큰의 속성

이 백서에 명시적으로 적용된 경우를 제외하고, 토큰은 BlackPearl 토큰과 관련해 어떠한 권리, 사용, 목적, 속성, 기능성 혹은 특징, 표현도 소유하고 있지 않으며, 암시, 포함, 제한 없음, 모든 사용, 목적, 속성, 기능성 혹은 특징을 가지고 있지 않습니다. BlackPearl 은 어떠한 경우에도 구매자에게 토큰이 권리, 사용, 목적, 속성, 기능성 혹은 특징을 가지고 있다고 나타내거나 보장하지 않습니다. 토큰의 구매는 구매자에게 어떠한 형태의 BlackPearl 혹은 BlackPearl의 총 수입이나 자산의 권리를 제공하지 않으며, 이는 모든 종류의 투표, 분배, 상환, 청산, 소유권(모든 형태의 지적 재산 포함), 혹은 기타 금융 관련 혹은 법적 권리를 포함하되 이에 국한되지 않습니다. 토큰의 구매는 BlackPearl에 대한 대출이 아닙니다. 또한 토큰의 구매는 구매자에게 어떠한 소유권 혹은 BlackPearl의 기타 이익을 제공하지 않습니다.

토큰은 환불 불가합니다.

BlackPearl은 어떠한 이유에도 구매자에게 환불을 제공할 의무가 없으며 구매자는 돈이나 기타 보상을 받게 되지 않을 것입니다. 토큰은 또한 구매자의 선택으로 상환될 수 없습니다. 이 백서에 제시된 진술은 단지 BlackPearl의 목표와 이러한 목표를 실현하기 위해 희망하는 작업 계획의 표현일 뿐이며, 토큰이 특정한 가치를 지니게 될 것이라는 데 대한 어떠한 보장도 없다는 약속을 포함하고 토큰에 관련하여 미래의 작업 수행 혹은 가격에 대한 어떠한 약속도 없습니다.

토큰은 ‘있는 그대로’ 제공됩니다.

토큰은 ‘있는 그대로’ 제공됩니다. 관련 당사자와 각 이사, 임원, 직원, 주주, 제휴사 및 면허인은 명시적, 묵시적, 법적 또는 기타와 관련하여 토큰과 관련된, 혹은 어떠한 종류의 대표나 보증도 하지 않으며, 또한 토큰과 BlackPearl 플랫폼이 방해받지 않는다거나, 오류가 없거나, 유해한 구성 요소가 없다거나, 안전하거나, 다른 방법으로 손실되거나 손상되지 않는 다는 어떠한 종류의 보증도 하지 않습니다. 관련 법률에 의해 금지된 범위를 제외하고, 관련 당사자와 각 이사, 임원, 직원, 주주, 제휴사 및 면허인은 상품성, 만족스러운 품질, 특정 목적에 대한 적합성, 침해되지 않거나 향유권 대한 묵시적 보증을 포함한 거래, 사용 또는 거래 과정에서 발생하는 어떠한 보증도 하지 않습니다.

토큰은 가치가 없을 수 있습니다.

토큰은 가치가 없을 수 있으며, 토큰의 유동성에 대해서 어떠한 보장이나 대표성도 없습니다. BlackPearl은 토큰의 시장 가치, 제 3자 혹은 그 외 어떠한 시장에서의 토큰의 양도성 그리고/혹은 유동성 그리고/혹은 가용성에 대한 법적 책임이 있거나 법적 책임을 져야 할 의무가 없습니다.

토큰 시장 개발 부족

토큰이 상장될 것이라는 데 대한 보증이나 토큰이 다른 암호화폐 그리고/혹은 법정 화폐로 교환 가능하다는 것에 대한 보증은 없습니다. 교환 시 토큰을 사용할 수 있는 경우, 그러한 교환은 규제 감독 대상이 될 수 없으며 BlackPearl은 교환 서비스 제공자와 관련하여 어떠한 보증도 하지 않는다는 점을 분명히 주의해야 합니다. 토큰의 이전 공개 거래 시장이 없었기 때문에 토큰 출시로 인해 토큰이 활성화 된다거나 유동 시장이 형성되지 않을 수 있으며 토큰의 가격은 변동될 수 있습니다. 토큰 보유자는 토큰을 쉽게 처분할 수 없을 수 있으며, 2차 시장이 발달하지 않는 경우, 토큰 보유자는 토큰을 전혀 청산할 수 없을 수 있습니다. 제안된 송신자가 BlackPearl의 KYC 및 AML 절차(신원 확인 및 자금 출처의 포함, 증명, 제한 없이)를 완료하지 않은 경우 어떠한 상황에서도BlackPearl 의해 토큰의 송금 제안이 차단될 수 있습니다. 구매자는 차후 판매에 대한 제약을 인식해야 합니다.

투기성이 높은 가격과 관련된 위험

2차 시장에서 암호화폐의 가치 평가는 보통 투명하지 않으며, 투기성이 높습니다. 토큰은 BlackPearl 자산에 대한 어떠한 소유권 권리도 보유하지 않으며, 그러므로, 어떠한 유형 자산도 반환되지 않습니다. 2차 시장에서 토큰의 가치는 짧은 시간 내에 크게 변동할 수 있습니다. 구매자들이 기여한 전체 수량을 모두 잃을 수 있는 상당한 위험이 있으며 최악의 경우, 토큰의 가치를 모두 잃을 수 있습니다.

불가항력

이 백서에 진술된 토큰 런칭 및 BlackPearl의 작업 수행 활동 및 개발 로드맵은 불가항력적인 상황으로 인해 중단, 일시 중단 또는 지연될 수 있습니다. 본 백서의 목적상, "불가항력"은 BlackPearl에 의해 예방될 수 없는 비상한 사건 및 상황을 의미하며, 다음을 포함합니다: 시장력 또는 기술, 자연 행위, 전쟁, 무력 충돌, 대규모 시민 난동, 산업 활동, 전염병, 사무실 폐쇄, 생산 지연, 에너지 공급 또는 통신 서비스의 장기적 부족 또는 기타 실패, 시, 주 또는 연방 정부 기관의 행위, 토큰 런칭 시 존재하지 않았던 BlackPearl의 통제를 벗어난 기타 상황.

보험

은행 계좌나 금융 기관의 계좌와는 달리, 구매자가 특별히 개인 보험을 들어 보호하지 않는 한 토큰은 보험의 적용을 받지 않습니다. 따라서 효용가치를 상실하거나 상실한 경우, BlackPearl이 구매자에게 상환청구권을 제공하기 위해 마련한 공적 보험자나 개인 보험은 없습니다.

정부 공시

BlackPearl은 규제된 뮤추얼 펀드가 아님 (Mutual fund)

BlackPearl은 케이맨 제도의 뮤추얼 펀드 법(2019년 수정)의 목적에 따라 뮤추얼 펀드로 규제되지 않으며 토큰이 공유되지 않음에 근거하여BlackPearl은 뮤추얼 펀드가 아닙니다. 또한, 토큰은 구매자의 선택에 따라 상환할 수 없으므로 토큰과 BlackPearl은 '폐쇄'된 것으로 간주합니다.

따라서, 이 백서의 사본이나 BlackPearl에 관한 세부 사항은 케이맨 제도 통화 당국("CIMA")에 제출되지 않았습니다. BlackPearl은 규제된 뮤추얼 펀드가 아니기 때문에 BlackPearl은 CIMA의 감독 대상이 아니며 BlackPearl은 해당 계정을 감사받거나 CIMA에 제출하지 않아도 됩니다.

BlackPearl이 MFL에 따라 뮤추얼 펀드로 규제되는 경우, BlackPearl은 투자자를 보호하기 위해 설계된 규제 요구사항을 준수해야 하며, 이는 토큰 구매 최소 총액을 미국달러 100,000달러 혹은 동등한 어떠한 종류의 통화로 제한하여 허가받은 뮤추얼 펀드 관리자에 의해 허가받거나 관리되지 않게 하기 위함입니다. BlackPearl은 규정된 초기 등록비 또한 지불해야 할 것입니다.

이러한 사항은 MFL에 따른 초기 등록과 관련하여 필요한 사항입니다. BlackPearl은 초기 등록 후 MFL에 따라 지속적인 의무를 갖게 될 것입니다. 이 백서의 모든 변경 사항을 CIMA에 보고하고, 승인된 감사인에 의해 감사된 CIMA 계정을 매년 제출하며, 기금 연간 수익금을 청구하고 규정된 연간 수수료를 지불해야 하는 의무가 포함됩니다.

만약 회사가 규제된 뮤추얼 펀드라면, 회사는CIMA의 감독 대상이 될 것이고, CIMA는 특정한 사건이 발생하면 특정한 조치를 취할 수 있는 광범위한 권한을 가질 것 입니다.

하나 혹은 하나 이상의 국가에서 불리한 규제 조치의 위험

암호 토큰, 디지털 자산 및 블록체인 기술의 규제 상태는 개발되지 않았고 국가마다 크게 다르며, 상당한 불확실성의 영향을 받고 있습니다. 특정 국가가 법, 규정, 정책 또는 규칙을 채택하여 비트코인과 이더리움 네트워크에 직간접적으로 영향을 미치거나, 토큰을 취득, 소유, 보유, 판매, 전환, 거래 또는 사용할 권리를 제한할 수 있습니다. 법률, 규정, 정책 또는 규칙의 개발은 토큰이 종속되는 블록체인 네트워크의 운영 특성을 변화시킬 수 있으며, 정부 당국이 관련 당사자들의 업무를 조사하거나 관련 당사자들에 대한 시행 조치를 추진하지 않을 것이라는 보장은 없을 수 있습니다. 이 모두는 관련 당사자들에게 판단, 합의, 벌금 또는 벌칙을 부과할 수 있고, 관련 당사자들이 운영과 활동을 재구성하거나 특정 제품이나 서비스의 제공을 중단하도록 할 수

있으며, 이 모든 것은 관련 당사자들의 명성에 해를 끼치거나 운영 비용을 증가시킬 수 있기에, 이는 결국 토큰 및/또는 BlackPearl 플랫폼 개발에 부정적인 영향을 끼칠 수 있습니다.

구매자는 법적 분류의 책임을 진다

토큰이 특정 국가에서 보안으로 간주될 수 있거나, 향후의 보안으로 간주될 수 있는 위험이 있습니다. BlackPearl은 토큰이 구매자의 국가에서 담보가 될 수 있다는 어떠한 보증 및 보장을 하지 않습니다. 각 구매자는 토큰이 구매자의 국가에서 담보가 될 수 있는지에 대한 결과를 감수해야 합니다. 모든 구매자는 토큰의 취득과 처분이 관련된 국가에서 합법적인지 확인해야 할 책임이 있으며, 각 구매자는 어떤 국가에서도 법을 토큰을 위법적인 행위에 쓰지 않아야 합니다. 구매자가 토큰의 구입이나 사용이 해당 관할구역에서 합법적이지 않다고 판단하는 경우(또는 회사가 등록이나 면허 등록 같은 추가 조치를 취한 경우에만 합법적임), 토큰을 취득하지 않아야 하고 토큰의 사용이나 소유를 즉시 중단해야 합니다.

암호화폐와 교환하여 토큰을 취득하는 것은 전 세계의 여러 규제 기관들에 의해 계속 조사될 수 있으며, 이는 토큰의 사용에 영향을 미칠 수 있습니다. 일부 국가에서 토큰을 제공하거나 지원하는 BlackPearl의 법적 능력은 향후 규제 또는 법적 조치에 의해 제거될 수 있습니다. BlackPearl이 토큰의 구매 또는 사용이 특정 국가에서 불법이라고 결정한 경우, BlackPearl은 해당 국가에서 운영을 중단하거나 적용 가능한 법률에 따라 토큰을 조정할 수 있습니다.

구매자는 양도 규제를 준수할 책임이 있다.

토큰은 제3자 거래소에 배치되어 미래의 구매자와 사용자에게 토큰을 구매 할 수 있는 기회를 제공할 수 있습니다. 토큰 런칭 후 BlackPearl 플랫폼에 참여하고자 하는 사용자는 BlackPearl 토큰이 배치된 거래소에서 토큰을 구입해야 합니다. 반대로, 토큰 보유자가 BlackPearl플랫폼 생태계에서 벗어나고자 한다면 토큰을 거래소에서 판매할 수가 있습니다. 미국, 중국, 대한민국, 캐나다, 싱가포르와 같은 특정 국가들의 유가증권 유통에 관한 기존 법률은, 해당 국가의

국민들에게 토큰의 판매를 금지할 수 있습니다. 토큰을 구매할 때 구매자들은 후속 판매에 대한 규제를 인식해야 합니다.

일반적인 보안 리스크

도난 및 해킹 위험

토큰 생성 관련된 행사와 ICO는 해커들의 표적이 됩니다. 해커들은 BlackPearl 플랫폼 및 구매자의 지갑, BlackPearl 스마트 컨트랙트 또는 여러 방면에서 토큰의 가용성에 관계없이 제한 없는 서비스 거부 공격, Sybil 공격, 위장 공격, 스머핑, 말웨어 공격 혹은 컨센서스 기반 공격을 포함한 모든 방법으로, 구매자의 디지털 지갑에 간섭을 시도 할 수 있으며, 이러한 공격은 구매자의 토큰이 도난 당하는 결과를 초래할 수 있습니다.

프라이빗 키

구매자에 의해 구매된 토큰은 구매자의 지갑 혹은 저장소에 보유할 수 있으며, 이에 접근하기 위해서는 프라이빗 키 혹은 프라이빗 키들의 조합을 요구합니다. 따라서, 구매자의 지갑 또는 저장소와 관련된 필요한 프라이빗 키(들)가 분실되면 해당 토큰의 손실을 초래할 수 있습니다. 더욱이, 어떠한 제 3자라도 지갑이나 저장소 서비스의 로그인 권리를 및 프라이빗 키(들)에 대한 접근을 얻는다면, 구매자의 토큰을 횡령할 수 있습니다. BlackPearl은 이러한 손실에 대해 어떠한 책임도 지지 않으며 손실에 대해 무해한 상태를 유지합니다.

구매자의 지갑에 퍼블릭 키 맵핑 실패

구매자가 지갑에 퍼블릭 키를 매핑하지 잘못할 경우, BlackPearl 플랫폼에 기반한 새로운 블록체인 초기 잔액을 구성할 때 제3자가 이더리움 블록체인에서 구매자의 토큰 잔액을 인식할 수 없게 될 수 있습니다.

호환되지 않는 지갑 서비스에 대한 위험

토큰의 획득 및 저장에 사용되는 지갑 또는 지갑 서비스 제공자는 토큰과 기술적으로 호환되어야 하며 이를 확신하지 못할 경우 이는 구매자가 자신의 토큰에 접근할 수 없는 상황을 초래할 수 있습니다.

암호학 분야의 약점이나 착취적인 돌파구의 위험

암호학의 발전이나 양자 컴퓨터의 발전과 같은 다른 기술적 발전은 암호화폐, 이더리움 및 토큰에 위험을 줄 수 있으며, 이로 인해 토큰이 도난 되거나 분실될 수 있습니다.

인터넷 전송 위험

하드웨어, 소프트웨어 및 인터넷 연결의 실패를 포함하여 토큰 사용과 관련된 위험이 있습니다. BlackPearl은 BlackPearl 플랫폼과 토큰을 사용 시 발생할 수 있는 통신 장애, 중단, 오류, 왜곡 또는 지연에 대해 어떠한 책임도 지지 않습니다. 암호화의 거래는 되돌릴 수 없으며, 따라서 사기 또는 우발적인 거래로 인한 손실은 회수가 불가능할 수 있습니다. 암호화폐 거래는 공공 원장에 기록될 때 이루어지는 것으로 간주되며, 거래가 개시된 날짜나 시간과 반드시 일치해야 할 필요는 없습니다.

BlackPearl 플랫폼 공시

BlackPearl 스마트 컨트랙트가 개발된다는 보장이 없습니다.

각 구매자는 다음과 같은 사항을 예상해서는 안 되며 BlackPearl에 의한 보장이나 대표 또는 보증이 없다는 것을 인정하고, 이해하며, 이에 동의합니다.

- BlackPearl 플랫폼이 언젠가는 채택될 것이다
- BlackPearl 플랫폼은 다른 형태나 수정된 형태가 아닌 BlackPearl에 의해 개발되어 채택된다.
- 블록체인 유틸라이징이나 BlackPearl 채택이 언젠가는 런칭될 것이다.
- BlackPearl 토큰의 사용이 가능해지거나 토큰과 교환이 가능해 질 것이다.

● BlackPearl플랫폼의 변화에 관계없이 또는 분배가 초기 코인의 고정된 잔고와 일치 혹은 불일치할 수 있는 경우가 발생하여도, 블록체인이 런칭될 것이다. (아래에 정의함)

또한 토큰 출시("초기 토큰")에 따라 초기에 생성된 토큰은 BlackPearl 플랫폼에 대한 어떠한 기능이나 권리도 없으며 초기 토큰을 보유하는 것은 BlackPearl 플랫폼이 런칭되고 BlackPearl 스마트 컨트랙트가 채택되어도, 보유자가 BlackPearl 플랫폼을 사용할 수 있거나 플랫폼에 사용된 토큰을 받을 수 있다는 보증, 표시 또는 보장할 수 없습니다.

BlackPearl 스마트 컨트랙트 및 관련된 소프트웨어 그리고/혹은 인프라와 관련된 리스크

BlackPearl 스마트 컨트랙트는 이더리움 블록체인에 기반이며, 이와 같이 어떠한 이더리움 프로토콜의 기능 불량 혹은 의도하지 않은 기능, 또는 예상치 못한 기능 때문에 토큰 및 BlackPearl 플랫폼이 의도하지 않은 방식으로 오작동할 수가 있습니다.

이더리움 블록체인은 오픈 소스 소프트웨어이며, BlackPearl 스마트 컨트랙트가 의도적인 혹은 의도치 않은 버그나 결점을 포함하여 토큰에 부정적인 영향을 끼치거나 토큰의 도난이나 손실 혹은 토큰에 접근 또는 조종할 능력을 손실할 리스크가 있습니다. 그러한 소프트웨어 버그 혹은 결점의 경우에, 해결법이 없을 수 있으며 토큰 소유주들은 어떠한 해결책, 환불 혹은 보상도 보장받을 수 없습니다.

이더리움 블록체인에서, 블록 생산 시간은 작업 증명에 의해 결정되므로 블록 생산은 무작위적인 시간에 일어날 수 있습니다. 예를 들어, 배포 기간의 마지막 몇 초 동안 BlackPearl의 수취인 디지털 지갑 주소로 전송된 이더는 해당 기간 동안 포함되지 않을 수 있습니다.

구매자는 이더리움 블록체인이 예상한 시간에 본인의 거래를 포함하지 않을 수도 있다는 것을 이해하며 이더, 비트코인 혹은 법정화폐 통화를 같은 날에 받을 수 없을 수도 있다는 것을 이해합니다.

이더리움 블록체인은 거래가 지연되거나 손실될 수 있는 주기적인 혼잡을 일으키는 경향이 있습니다. 어떠한 개인들이 이더리움 네트워크를 의도적으로 스팸 발송을 하고 암호화폐 토큰을 구매하여 이득을 얻으려고 시도할 수도 있습니다. 구매자는 이더리움 블록 생산자들이 구매자의 거래를 원하는 시간 또는 거래를 아예 포함하지 않을 수 있다는 것을 인정하고 이해합니다.

이더리움 블록체인 어카운트의 본래 유닛인 이더는 토큰과 비슷한 방법으로 가치를 잃을 수 있으며, 다른 방식으로도 가치를 잃을 수 있습니다. 이더리움에 대한 더 자세한 정보는 http://www.ethereum.org에서 찾을 수 있습니다.

철회 불가능한 블록체인 거래의 특성

블록체인에 블록으로 기록된 토큰과 관련된 거래는 일반적으로 해제할 수 없습니다. 거래가 오류로 판명되거나 사용자의 토큰이 도난 당하더라도, 거래는 되돌릴 수 없습니다. 현재, 분실 또는 도난 암호화폐와 디지털 토큰에 관한 조치나 불만을 제기할 수 있는 정부, 규제, 수사 또는 검사 권한이나 메커니즘이 없으므로, BlackPearl은 누락된 토큰을 교체하거나 토큰의 잘못된 양도 또는 도난을 대체할 수 없습니다.

프로토콜 수정

이더리움 블록체인 혹은 BlackPearl 스마트 컨트랙트의 자원 코드의 개발 팀과 관리자들은 네트워크 프로토콜과 소프트웨어에 대한 수정을 네트워크 커뮤니티에 의해 수용되고 승인되거나, 혹은 수용되지 않더라도 제안할 수 있으며, 토큰의 공급, 보안, 가치 혹은 시장 공유에 반대 영향을 끼칠 수 있습니다.

채굴 공격 위험

토큰으로 사용되는 이더리움 블록체인은 다른 탈중앙화 암호화폐와 같이 채굴 공격, 이중 사용 공격, 다수 채굴 동력 공격, "이기적인 채굴" 공격, 경쟁 조건 공격을 포함하지만 이에 국한되지 않는 공격에 민감합니다.

성공적인 공격은 토큰에 위험을 초래하고, 토큰의 적절한 실행, 시퀀싱과 일반적으로 이더리움 계약 연산의 적절한 실행 및 중단이 예상됩니다. BlackPearl과 이더리움 파운데이션의 노력에도 불구하고, 이미 알려진 또는 새로운 채굴 공격은 존재합니다. 채굴 공격은 위에 언급했듯이, 다른 블록체인 네트워크를 타깃으로 삼을 수 있으며 토큰과 상호작용을 하는 다른 블록체인 네트워크를 목표로 할 수 있으므로 결과적으로 토큰은 위에서 설명한 범위까지 이러한 방법으로도 영향을 받을 수 있습니다.

Player 또는 Club에 의한 채무 불이행의 위험

BlackPearl 토큰 및 토큰의 보유와 관련하여 구매자에게 지급되는 모든 종류의 돈, 자금 혹은 토큰은 Player 또는 Club이 의무를 수행하는 것에 의존하며, BlackPearl 스마트 컨트랙트에 의한 BlackPearl 토큰 분배의 소유주들에게 이러한 돈, 자금 혹은 토큰을 보장합니다. 이 Player 또는 Club이 채무 불이행을 할 위험이 있으며, 구매자는 BlackPearl 토큰의 보유와 관련해서 아예 지불 받지 못할 수 있습니다. 이러한 행동은 BlackPearl 플랫폼과 그 가치 그리고/혹은 본인이 소유한 모든 토큰의 유틸리티에 악영향을 끼칠 수 있습니다.

BlackPearl 토큰 소유자는 Player, Club에 의해 일어난 채무 불이행에 대한 법적 절차를 선동할 수 있는 계약상의 관계 또는 능력이 없을 수 있으며, 토큰 및 BlackPearl 토큰을 취득하기 전에 이러한 상황에 특정한 법적 고문을 받아야 합니다.

또한, 구매자가 BlackPearl 토큰 취득으로 지원하기로 선택한 Player, Club은 그들의 잠재력을 실행 혹은 성공하거나 구매자에게 보상을 되돌려 줄만큼 충분히 대가를 받지 못할 수도 있습니다
.

회사 공시

토큰 생성기의 법적 구조

BlackPearl은 케이맨 제도의 기업 법(개정된)에 따라 케이맨 제도에 법인화된 면제 회사입니다. 면제 회사란 기업의 이익에 관한 어떤 질문에도 불구하고, 자연인의 모든 기능을 발휘할 수 있는 별도의 법적 성격을 가진 기업이며, 영속계승권을 가지고 있습니다. 면제 회사의 헌법은 두 문서에

포함되어 있으며, 회사 설립 계약서 및 회사 정관에 나와있습니다. (이하 "정관") 정관은 케이맨 제도 회사의 이사가 적어도 한 명은 있어야 한다고 규정하고 있으며 일반적으로, 정관은 케이맨 제도의 경영관리가 이사회에 의해 수행되고 이사회에 책임이 있다고 명시하고 있습니다. 이 조항이 허용하는 경우, 케이맨 회사는 회사의 임원과 이사에 대해 모든 법적 책임과 그들의 임무 수행 중 사람을 찾음으로써 초래되는 비용을 면책할 수 있습니다.

케이맨 제도 회사 정관은 그러한 회사의 승인 받은 주식 자본을 명시해야 합니다. 정관은 승인된 주식 자본의 총액과 분배된 주식의 숫자 세부사항 및 그 주식의 액면 가치에 대한 세부사항을 명시할 것입니다. 토큰 소유자로서, 본인은 회사 설립 계약서 혹은 정관의 당사자가 아니며 BlackPearl 주식에 어떠한 권리 혹은 이득에 대한 자격도 없으며, BlackPearl 이사회를 임명하거나 제거할 권리가 없습니다.

토큰은 BlackPearl 플랫폼 또는 BlackPearl과 관련하여 어떠한 종류의 지배권도 부여하지 않기 때문에 BlackPearl 플랫폼 내의 혹은 BlackPearl자체의 제품 또는 서비스와 관련된 모든 결정은 BlackPearl이 단독으로 결정할 것입니다. 이 결정은 BlackPearl 플랫폼 혹은 그 가치 그리고/혹은 본인이 소유한 모든 종류의 토큰 유틸리티에 악영향을 끼칠 수 있습니다.

경영진에 의존

BlackPearl 플랫폼을 경쟁력있는 위치에 유지할 책임이 있는 BlackPearl 플랫폼 경영진의 능력은 고위 경영 팀의 서비스에 크게 의존합니다. 그러한 고위 경영진 구성원들의 서비스 손실 또는 감소 또는 추가적인 고위 경영진 유인, 유지 및 유지 불능은 BlackPearl 플랫폼과 토큰의 가치에 중대한 악영향을 미칠 수 있습니다. 자격이 있는 개인의 수가 적기 때문에, 관련된 전문가들의 경쟁이 심하며 이 경쟁은 BlackPearl의 기존 고위 경영을 유지할 능력에 악영향을 미칠 수 있으며 자격 있는 고위 경영인을 추가적으로 유인하는 것은 BlackPearl 플랫폼과 토큰의 가치에 큰 악영향을 끼칠 수 있습니다.

제3자에 대한 의존과 관련된 위험

완료되더라도 BlackPearl 플랫폼은 전체 또는 부분적으로 제3자에 의존하여 채택 및 구현하고 이를 지속적으로 개발, 공급 및 지원할 것입니다. 제 3자가 그들의 작업을 완료하거나, 의무를 적절히

수행하거나, 누군가의 요구를 충족하는 것을 보장하거나 보증하는 것은 없습니다. 이 또한BlackPearl 플랫폼과 토큰의 가치에 큰 악영향을 끼칠 수 있다.

BlackPearl 플랫폼과 토큰에 대한 불충분한 관심

BlackPearl과 토큰이 다수의 개인이나 비즈니스, 기관에 의해 사용되지 않을 수도 있으며 그 기능을 창조 또는 발전시키는데 공공의 관심이 제한될 수 있습니다. 그러한 관심의 부족은 BlackPearl 플랫폼과 토큰의 가치 발전에 영향을 끼칠 수 있습니다.

플랫폼 발전 리스크

BlackPearl 플랫폼 그리고/혹은 BlackPearl 스마트 커트랙트의 발전은 공공의 관심 부족, 자금 부족, 상업적 성공 혹은 전망 부족과 같은 이유로 폐기될 수 있습니다.

BlackPearl 플랫폼 변화

BlackPearl 플랫폼은 아직 개발 중이며 시간을 거쳐 상당한 변화가 일어날 수 있습니다. 관련 당사자들은 BlackPearl 플랫폼이 본 백서에 명시된 특징과 사양을 갖기를 의도하지만, 그러한 특징과 사양에 대한 변경은 여러 가지 이유로 이루어질 수 있으며, 이는 BlackPearl 플랫폼이 구매자의 기대를 충족하지 못한다는 것을 의미할 수 있습니다.

기타 프로젝트

BlackPearl 플랫폼은 관련 당사자들과 제휴하거나 무관한 당사자들에 의해 추진되는 다른 대안적인 프로젝트를 야기할 수 있으며, 그러한 프로젝트는 BlackPearl 플랫폼에 아무런 이득도 제공하지 않을 수 있습니다.

이해 충돌과 관련된 공시

관련 당사자들 중 누구라도 관련 당사자들과 거래를 할 수 있고 이해 상충이 발생할 수 있으며, 잠재적으로 시장의 힘에 의해 결정되지 않은 조건에 따른 거래 결과를 초래할 수 있습니다.

구매자에 의한 승인 및 보증

승인

(i) 본 백서(또는 그 일부)의 정보 소유에 대한 접근 또는 수용 또는 (ii) 지급을 이전(법정 화폐 또는 암호 화폐)하고 토큰 구매에 동의함으로써, 각 구매자는 다음 사항에 동의하고 인정합니다.

● 토큰은 어떤 국가에서도 유가 증권으로 구성되지 않으며 그렇게 의도되지 않는다. 본 백서는 어떤 종류의 제안서나 다른 어떤 조율의 문서도 구성하거나 제안하지 않으며, 어떤 국가에서도 유가 증권에 대한 투자를 간청하거나 유가증권 제안을 구성하도록 의도되지 않는다.

● 토큰은 BlackPearl 플랫폼 내부에서 사용되도록 만들어졌으며 투기 거래 목적으로 사용되는 다른 자산이나 유가증권으로 의도되지 않는다. BlackPearl은 토큰의 거래를 수행하지 않으며 토큰의 미래 가치에 대해 보증하지 않는다. BlackPearl은 제 3자를 통한 어떠한 종류의 토큰 거래에 대한 책임도 없다. 토큰이 아무 가치도 가질 수 없을 가능성이 존재한다.

● 이 백서는 토큰 구입 또는 판매에 대한 조언 또는 토큰 구매 제안에 대한 어떠한 요청도 구성하거나 의견의 일부를 형성하지 않는다. 또한, 계약, 투자 또는 구매 결정의 기초 또는 그 일부 또는 그 표시의 사실이 어떠한 계약 또는 투자 또는 구매 결정의 기초가 되거나 이 사실에 의존할 수 없다.

●해당 관할권의 어떤 규제 당국도 본 백서에 명시된 정보를 조사하거나 승인하지 않았으며, 본 백서의 발행, 배포 또는 배포는 해당 법률, 규제 요건 또는 규칙이 준수되었음을 의미하지 않는다.

● BlackPearl과 구매자, 그리고 토큰의 판매와 구매와 관련하여 계약은 구매 문서가 없는 경우 이 백서의 적용을 받는다.

●본 백서의 다른 섹션에도 불구하고, 그리고 해당 법률에 의해 허용되는 범위에도 불구하고, BlackPearl은 구매자에 의한 본 백서 또는 그 일부에 대한 수락 또는 의존에서 발생하는 불법, 계약 또는 그 밖의 다른 유형(수익, 수익 또는 이익, 사용 또는 데이터 손실 포함하나 이에 국한되지 않음)의 간접적, 특수, 부수적, 결과적 또는 어떠한 종류의 손실, 불법 행위, 계약 혹은 기타 손실에 대해 책임을 지지 않는다.

● 백서의 어떤 정보도 BlackPearl, 토큰 및 토큰 런칭과 관련된 비즈니스, 법적, 재정 혹은 세금 관련 조언으로 간주되지 않아야 한다.

● 또한 BlackPearl과 그 각각의 사업과 운영, 토큰과 토큰 론칭에 관해 그들 자신의 법률, 재정, 세금 또는 다른 전문적인 조언자와 상의해야 한다.

토큰 모델 승인 및 보증

보증

(i) 본 백서(또는 그 일부)의 정보 소유에 대한 접근 또는 수용, 또는 (ii) 지급을 이전(법정 화폐 또는 암호화폐)하고 토큰 구매에 동의함으로써, 각 구매자는 BlackPearl에 다음 사항을 대표하고 보증합니다.

● 본 백서에 명시된 토큰 출시 및 토큰 구매에 내재된 공시 및 공시되지 않은 위험, 거부권 및 기타 공시에 대한 단독 책임을 읽고 이해하며 수용한다.

●토큰의 판매 또는 배포가 불법(각각 "금지된 영토")인 국가 또는 구역의 시민 또는 거주자가 아니며, 금지 구역의 시민을 대신하여 토큰을 구입하지 않는다.

● 이 백서에 따라 이 백서에 접근, 배포, 전파를 포함하여 구매자의 의무를 따르고 수행하며 권리를 행사하고 관여할 수 있는 힘이 있으며, 이와 같은 행위가 구매자의 관할권 혹은 거주 국가의 해당하는 법, 규제, 규칙에서 금지되거나 제한되지 않았으며 언급된 바와 관련된 제한이 적용되는 경우 구매자는 다음과 같이 처리한다:

● 구매자는 구매자의 관할권 또는 거주 국가의 해당 법률, 규정 및 규칙을 준수하지 않을 경우 단독으로 책임을 진다.

● 또한, 구매자 관할권 또는 거주 국가의 모든 해당 법률, 규정 및 규칙을 구매자 자신의 비용과 단독 비용으로 준수하며 따른다.

● 모든 조치, 조건 및 필요한 사항을 구매자 자신의 단독 비용으로 처리하고, 단독으로 이행하며 완료한다.

● 이는 구매자가 합법적으로 관여하며, 그들의 권리를 행사하고 수행하며 이 백서에 도입된 그들의 의무를 준수하기 위함이며 이 의무가 법적으로 구속력이 있거나 효력을 가짐을 확실히 하기 위함이다.

● 이 백서에 진술된 토큰의 조건 문제는 구매자에 의해 처리, 실행되고 완료된다.

● 이 백서 내의 구매자의 의무는 유효하며, 구매자 조건에 따라 그러한 구매자에 유효하고, 구속력이 있으며, 효력이 있다. 이 조건은:

● 구매자는 작업, 기능성, 사용, 스토리지, 트랜스미션 메커니즘 및 기타 암호화폐에 대한 물질적 성격, 블록체인 기반 시스템, 암호 화폐 지갑 및 기타 코인 및 토큰 스토리지 메커니즘과 관련된 것들, 블록체인 기술 및 스마트 컨트랙트 기술에 대해 적절히 이해한다.

[page 53]

● 구매자는 다른 사람에게 토큰을 전달하려는 목적이나 한 거래를 완료하려는 의도의 여러 관련된 단계에서 토큰을 투기 투자 혹은 한 형태의 가상 화폐를 다른 형태로 바꾸려는 목적으로 암호화폐와 거래하지 않는다.

● 구매자는 토큰을 주로 BlackPearl 플랫폼에서 사용하기 위해 취득한다.

● 위의 모든 표현과 보증은 구입자의 사전 등록(해당하는 경우) 및 토큰 출시에 따른 토큰 구매 시점부터 진실되며, 완전하고, 정확하며, 오해의 소지가 없다.

기타 고지

AML 및 KYC

돈 세탁이나 테러리스트 자금을 방지하기 위한 목적으로 구매자의 신원 확인 그리고/혹은 BlackPearl에 있는 자금의 원천을 입증하도록 요구됩니다. 이 과정은 (i) 최초 토큰 구매, (ii) BlackPearl 플랫폼 사용, (iii) BlackPearl 토큰과의 교환, (4) 토큰 전송, (5) BlackPearl 토큰을 BlackPearl 스마트 컨트랙트를 통해 수신 혹은 (vi) BlackPearl이 AML 및 KYC 정책 및 과정과 관련이 및 필요가 있다고 간주되는 것들에 적용될 수 있습니다.

예를 들어, 개인은 공증인, 경찰, 거주국 대사 등과 같은 공증인 또는 공증인이 적법하게 인증한 원본과 함께 공증인 또는 신분증명서를 작성하도록 요구될 수 있다. 기업 신청자의 경우, 사업자 등록증(혹은 다른 이름)과 회사 정관(또는 이와 동등한 것)의 인증된 사본, 그리고 모든 이사 및 수익 유자의 이름과 거주지 및 사업 주소가 요구될 수 있습니다.

위에 언급된 세부사항은 BlackPearl이 예상 구매자의 자금의 원천을 증명하고 확인하는 것이 필요하다고 간주될 때 BlackPearl은 해당 정보 및 문서를 요청할 수 있습니다.

각 구매자가 BlackPearl이 요구하는 정보와 문서를 제공하지 못한 결과로 발생하는 손실에 대해 BlackPearl은 책임이 없습니다.

각 구매자는 자금 세탁 및 테러 자금 조달의 방지에 목적을 둔 조치와 관련하여 BlackPearl의 요청을 준수하지 않을 경우 토큰을 포함하지만 이에 국한되지 않고, BlackPearl 플랫폼 계좌 혹은 토큰의 철회 및 중단을 포함한 구매자에 대한 조치를 야기할 수 있음에 승인하고 동의합니다.

참고 문헌

[1] Honey badger BFT protocol 허니뱃저 비잔틴 장애 허용 프로토콜:
https://eprint.iacr.org/2016/199.pdf
[2] Ethash-PoW Ethash 작업증명:
https://github.com/ethereum/wiki/wiki/Ethash
[3] Merkle patricia tree 머클 패트리샤 트리:
https://github.com/ethereumjs/merkle-patricia-tree
or 또는:
https://github.com/ethereum/wiki/wiki/Patricia-Tree