WHITEPAPER

Data Ecosystem on Chain

Important Notice

This document (the “Whitepaper”) has been prepared by DREP Foundation Ltd. (“DREP Foundation”) and this notice is intended to address all readers who view or access it on any communication channel or platform. The Whitepaper is presented strictly for information purposes only, and shall not, under any circumstances, be treated as an offer of securities or an invitation to participate in any regulated investment scheme, howsoever defined in any jurisdiction around the world. In addition, none of the information contained herein is intended to form the basis of any advice or inducement to engage in any sort of investment activity.

This version of the Whitepaper is released as a draft for discussion and pre- information purposes only. This Whitepaper remains a work in progress and is subject to change without notice. Please do not copy or disseminate any part of this document without including this disclaimer and the section titled “Risks and Disclaimers”.

You are strongly encouraged to read the entire Whitepaper and familiarize yourself with all the information set out below, particularly in the section entitled “Risks and Disclaimers”. Please seek independent advice from your professional advisors, including lawyers, tax accountants and financial advisors, if you have any uncertainty or doubt as to any of the matters presented.

Please take note that you are not eligible and you are not to purchase any tokens in the token sale of the DREP Tokens by DREP Foundation (the “Token Sale”) if:
(a) you are located in the People’s Republic of China or if you are a citizen or resident (tax or otherwise) of, or domiciled in, the People’s Republic of China;
(b) you are located in the United States of America or if you are a citizen, resident (tax or otherwise) or green card holder of, or domiciled in, the United States of America;
(c) such token sale is prohibited, restricted or unauthorized in any form or manner whether in full or in part under the laws, regulatory requirements or rules in any jurisdiction applicable to you, at the time of your intended purchase or purchase of the DREP Tokens in the Token Sale.

The Chinese version of the Whitepaper is the principal official source of information for DREP Foundation, if the content of the Whitepaper is lost, damaged or misinterpreted during the process of translation or communication, especially when translated to other languages including this English version, the Chinese whitepaper shall prevail in the event of any conflicts or inconsistencies.
Please note that this Whitepaper will be updated continuously and you are encouraged to review the Whitepaper on a regular basis

개요

인터넷을 상용화하는 이유가 정보를 연결하는 것이라면 블록체인이 인터넷과 인터넷을 통과 할 수 있는 이유는 데이터 장벽을 깨고 모든 것을 연결하기 때문이라고 말할 수 있습니다. DREP은 블록체인 기술에 "커넥터"와 "툴박스"를 구축하여 사용 편의성, 유연성 및 무 마찰 통합을 결합한 솔루션을 제공하기 위해 노력하고 있습니다.

현재 블록체인 채택은 여전히 분리 중이며 데이터는 여전히 분리 상태에 있습니다. 일반 퍼블릭 체인과 수직 산업 체인은 모두 경쟁 우위를 극대화하기 위해 폐쇄적인 생태계를 구축합니다. 그 결과, 더 많은 사용자에게 접근하기 위해 DApps(Decentralized Applications)는 서로 다른 퍼블릭 체인에 대한 독립 버전을 개발해야 하므로 사용자와 데이터 기반이 분리됩니다. 이 문제를 해결하기 위해 DREP은 탈중앙화 ID, 크로스 체인 구조 및 DREP SDK를 "커넥터"로 사용함으로써 동형 암호화에 기반한 데이터 공유에서 원-클릭, 크로스 플랫폼 데이터 통합 및 개인 정보 보호를 지원합니다.

블록체인이 연구소에서 실제 애플리케이션 및 대규모 채택으로 이동함에 따라 기업은 대개 블록체인에 대한 지식이 부족하여 기존 운영 환경에서 이 기술의 잠재적인 사용을 파악할 수 없습니다. 이 단계에서는 인프라 계층이든 애플리케이션 계층이든, 시장을 빠르게 침투하여 비즈니스 조각화의 문제점을 해결하려면 가볍고 고품질 제품화된 솔루션이 많이 필요하므로 원하는 기술 입력 출력 비율을 획득하고 사용자 환경을 극대화해야 합니다. 이러한 점에서, "툴박스"로 기능하는 DREP은 다양한 수직에 맞춘 DREP SDK뿐 아니라 맞춤형 이중 계층 아키텍처와 고급 API 및 플러그인 지원을 채택합니다.

간단히 말해서, DREP의 사명은 다음과 같습니다.

- 높은 동시성뿐만 아니라 더 이상 병목 현상을 일으키지 않도록 해야 합니다.
- 고객 지향 서비스뿐만 아니라 B측 및 C측 사용자가 무 마찰 방식으로 블록체인 서비스를 사용할 수 있도록 합니다.
- 상용화뿐만 아니라 격리된 모든 데이터베이스를 연결합니다.

DREP 정의

DREP은 사용 용이성, 유연성 및 마찰 없는 통합을 결합한 솔루션을 제공하는 블록체인 기술을 기반으로 하는 "커넥터" 및 "툴박스"를 개발하기 위해 노력합니다. DREP 체인, DREP ID, DREP 평판 프로토콜 및 DREP SDK를 기반으로 DREP은 체인에 퍼블릭 데이터 체인 생태계를 구축하여 퍼블릭 체인 생태 데이터의 격리된 현황을 깰 수 있습니다.

블록체인 기술은 오늘날까지 발전하고 있으며, 한편으로 계속해서 블록체인 프로젝트는 확장가능성, 안전성 및 프라이버시 등의 측면에서 끊임없이 솔루션을 제공하였지만, 여전히 규모가 제한적이고 유형도 부족하며, 소수의 응용 프로그램에만 서비스를 제공할 수 있습니다. 반면 대규모 기업에서는 블록체인 기술을 대량으로 채택하는 경우가 거의 없으므로 새로운 사용자를 확보하는 것이 더 어려워집니다.

DREP은 그 이유 때문에 다음과 같은 세 가지 문제를 해결하기 위해 노력합니다.
- 퍼블릭 체인의 성능이 부족하고 개발자 경험이 부족합니다.
- 블록체인 기반의 퍼블릭 체인 생태계 시스템과 소규모 사용자 기반을 분리합니다.
- 블록체인 기술과 기업의 요구사항이 일치하지 않습니다.

DREP은 주로 다음과 같은 기술적 솔루션을 제공합니다.

- DREP Chain은 DREP 팀이 완전히 개발한 고성능 퍼블릭 체인입니다. 루트 체인 및 맞춤형 서브 체인으로 구성된 이중 계층 구조로 EVM 및 WASM 형식의 스마트 계약(Smart Contract)과 호환됩니다.
- DREP 팀에서 혁신적으로 제안한 스마트 파이프라인은 데이터 전송 향상 및 블록체인 가상 시스템과 외부 응용 프로그램 간의 데이터 전송을 위한 "파이프라인"입니다. 보안에 영향을 미치지 않으면서 고효율, 제로 가스 소비 및 강력한 확장성을 달성할 수 있습니다. 이러한 현실적인 요구는 스마트 계약의 사용으로 해결되지 않았습니다.
- DREP은 네트워크 효율성을 높이고 전송 부담(overhead)을 줄이기 위해 Secp256k1 타원 곡선을 기반으로 하는 Schnorr 멀티 서명 알고리즘을 채택합니다.
- 데이터 연결 및 개인 정보 보호를 위해 DREP은 HMAC (해시 메시지 인증 코드) 알고리즘을 기반으로 하는 탈중앙화 ID 시스템을 설계하여 마스터 ID와 여러 서브 ID의 이중 계층 시스템을 구성합니다. DREP 클라이언트는 사용자가 탈중앙화 및 중앙화 플랫폼에서 한 번에 데이터 및 자산을 관리할 수 있게 합니다.
- 데이터 프라이버시 보호를 강화하기 위해 DREP은 준 유사 암호화를 사용하여 사용자가 개인으로 식별 한 정보를 처리합니다.

• DREP DID의 장기 보유 가치를 제공하기 위해 DREP은 평판 시스템을 시작했습니다. 이것은 일반적인 평판 프로토콜, 평판 파이프라인 인터페이스, 평판 데이터와 체인 및 알고리즘 라이브러리, 평판 인센티브 메커니즘, 평판 계정 관리 및 허위 계정 식별 메커니즘 등으로 구성됩니다.
• 기술 사용의 한계와 학습 비용을 낮추기 위해 DREP은 여러 가지 수직 계열에 대한 API, 플러그인 및 SDK를 개발했습니다. 이러한 툴박스를 통해 DApp R & D 팀은 원-클릭으로 멀티 퍼블릭 체인 자산 버전, 지갑 및 자산 거래 플랫폼을 출시 할 수 있습니다. DApp R & D 팀은 DREP ID를 기반으로 보다 많은 퍼블릭 체인 사용자를 확보하고 다양한 디지털 자산 소유자를 애플리케이션 사용자로 전환하고 Super DApps를 생성 할 수 있습니다.
• DREP 코드 스타일은 Java의 Spring 컨테이너 개발과 유사한 서비스 지향 프로그래밍입니다. 대부분의 블록체인 프로젝트 코드에서는 모듈 간의 커플링(coupling)이 더 심각합니다. 이 방식을 사용하면 DREP를 통해 모듈을 완전히 분리할 수 있으며 보다 명확한 논리로 코드를 쉽게 리팩토링(refactore) 할 수 있습니다.

DREP 메인 네트워크가 공식 발표되기 전에 DREP 테스트 네트워크는 4개의 버전을 거치며 각각 개발 팀을 대표하는 4개의 중요한 작업 절로 DREP 제품, 시장 및 비즈니스 팀을 대표하여 협력업체와의 커뮤니케이션 과정에서 지속적으로 문제를 발굴하고 솔루션을 제공할 것입니다. DREP의 4개의 테스트 네트워크는 각각 Darwin, Riemann, Euler, Planck의 발전을 상징하는 과학자로 명명됩니다.

- **Darwin** **The Evolutional Origin**
- **Riemann** **The Breaking Point**
- **Euler** **The Eternal Method**
- **Planck** **The Constant Change**

DREP Solutions

2.1 퍼블릭 체인의 성능 부족, 개발자 체험 부족

TPS(Transactions Per Second)는 퍼블릭 체인 채택의 주요 제한 사항 중 하나입니다. 서드 파티 지급 Paypal은 현재 100 TPS를 자랑하며 Visa는 최대 2000TPS까지 처리할 수 있습니다. 반대로 비트코인과 Ethereum은 10 TPS만 처리할 수 있어 블록체인 지급을 제한할 뿐 아니라 DApp을 만드는 것이 어려워집니다.

DApp의 지속적인 개발로 인해 이를 통해 처리되는 온-체인 데이터의 양이 큰 폭으로 증가했습니다. 예를 들어 EOS의 RAM은 이미 사용률이 62%에 달하고 있으며, 사용률과 자원 비용은 시간이 지남에 따라 지속적으로 증가하기 때문에 퍼블릭 체인 플랫폼의 확장이 더욱 어려워졌습니다. 또한 동시성 문제를 고려할 때 DApp 데이터를 기록하기 위해 프로토콜 계층 스마트 계약에만 의존하는 것은 불가능합니다.

탈중앙화, 확장성 및 보안이 모두 충족될 수 없는 Imposible Blockchain Triangle이 있습니다. 이는 퍼블릭 체인이 탈중앙화 보안을 희생하지 않고서는 TPS를 개선할 수 없다는 것을 의미합니다. DREP은 '스마트 파이프라인'이라고 불리는 확장성을 개선하기 위한 대체 방법을 제안했습니다. Layer 2솔루션과 마찬가지로 일괄적으로 데이터 처리 용량을 개선하고 맞춤형 개발 도구를 제공하여 퍼블릭 체인 확장성의 병목 현상을 해소할 수 있습니다.

2.1.1 DREP Smart Pipeline은 데이터 처리 용량을 일괄적으로 개선합니다.

스마트 파이프라인(Smart Pipeline)은 DREP 팀이 제안한 혁신적인 블록체인 애플리케이션 모델입니다. 보안에 영향을 미치지 않고 높은 효율성, 제로 가스 소비 및 강력한 확장성을 달성할 수 있습니다.

이러한 현실적인 요구 사항은 스마트 계약 사용으로 해결되지 않았습니다.
스마트 계약은 Ethereum과 같은 플랫폼에서 널리 사용되고 있지만, 데이터 용량, 가스 소비량 및 활성 통화 기능(Active Calling Function)의 부족은 개발자들에게 비난을 받고 있습니다. 이는 대규모 DApp의 개발을 효과적으로 제한합니다.

DREP 스마트 파이프라인은 데이터 전송 및 블록체인 가상 시스템과 외부 애플리케이션 간의 데이터 전송을 위한 "파이프라인"입니다. 블록체인 클라이언트는 스마트 파이프라인을 통해 외부

애플리케이션으로 실시간 데이터를 전송하고 외부 애플리케이션은 스마트 파이프라인을 전달하기 전에 결과를 실행한 후 데이터를 블록체인 클라이언트로 실시간으로 반환합니다. 외부 애플리케이션은 집행한 결과를 스마트 파이프라인을 거쳐 실시간으로 블록체인 클라이언트로 반환합니다.

스마트 파이프라인은 모든 프로세스에 삽입할 수 있으며 선택한 인서터의 위치에 따라 해당 코드를 실행하여 실행 효율성을 높일 수 있습니다.

스마트 파이프라인의 장점은 다음과 같습니다.

- **"Smarter":** 스마트 파이프라인을 체인에 배치한 후에는 세부 조건에 따라 자동으로 트리거 할 수 있습니다. 스마트 계약과 비교하면 더 많은 조건을 고려할 수 있으며 실행 프로세스가 방해받기가 더 어려워질 수 있습니다. 이것은 복잡한 트랜잭션의 실행에 도움이 됩니다.
- **Zero gas consumption:** 스마트 파이프라인을 사용하는 어플리케이션이 트랜잭션을 실행할 때 가스가 필요하지 않습니다. 그러나 제로 가스 소비가 책임을 질 필요가 없다는 것을 의미하는 것은 아니며 코드를 실행하는 모든 스마트 파이프라인에는 공개 소스 감독이 필요합니다. 또한 스마트 파이프라인이 지시하는 컴퓨팅 리소스 본문은 해당 서브 체인에서 찾을 수 있을 뿐만 아니라 스마트 파이프라인 코드에서도 찾을 수 있습니다. 따라서 허점이 있더라도 해당 서브 체인의 성능에는 영향을 미치지 않습니다.
- **No limitation in programming language**: 스마트 파이프라인은 WASM 가상 시스템을 사용하여 트랜잭션을 실행합니다. 사용자는 서로 다른 프로그래밍 언어로 코드를 작성한 다음 WASM 커맨드로 변환할 수 있습니다. WASM 이 계속 개선됨에 따라 지원되는 언어의 유형이 점차 증가하게 되며, 블록체인의 실행에 영향을 미치지 않고 코드 효율도 향상됩니다.
- **Meets the needs of complex applications:** 스마트 파이프라인 애플리케이션은 가스에 의해 제한되지 않으며 블록체인에서 지원되므로 보다 복잡한 논리를 구현할 수 있습니다. 스마트 파이프라인을 사용하는 블록체인은 다른 애플리케이션 또는 서비스와 상호 작용하여 대규모의 복잡한 애플리케이션의 요구사항을 충족할 수 있으므로 기존 블록체인이 지원하지 않는 애플리케이션을 구축할 수 있습니다.

2.1.2 DREP dual-layer architecture and customizable sub-chain

DREP 체인은 메인 체인과 서브 체인으로 구성된 dual-layer 구조로 형성되어 보안이나 분산에 영향을 미치지 않고 확장성을 개선하고 블록체인 인프라의 효율성을 향상시킵니다. DREP의 오픈 소스 테스트넷에서, DREP 체인 TPS는 2019년 1월 8일 공개 테스트 동안 최고점에서 12,000을 초과했습니다.

테스트 환경 조건은 다음과 같습니다.

- Block time: 10 seconds - 15 seconds
- Block size: No limit
- Structure: 1 main chain, 10 sub-chains.
- The structure of each chain: 7 mining nodes, 10 common nodes.
- Testnet address: drep.me

DREP 메인 체인과 서브 체인은 서로 다른 트랜잭션을 독립적으로 처리할 수 있으므로 여러 컨센서스 메커니즘을 서로 다른 데이터 저장소와 공존시키고 동시성을 향상시키며 다양한 응용 프로그램에서 액세스에 대한 호환성 지원을 제공할 수 있습니다. 따라서 블록체인 응용 프로그램, 전통적인 엔터프라이즈와 플랫폼을 도킹하든 해당 서브 체인을 사용자 정의하여 엑세스 장벽을 줄일 수 있습니다.

2.1.3 DREP 개선된 일치 메커니즘

PBFT는 하이퍼링거와 같은 컨소시엄 체인에 적용된 안전하고 효율적인 컨센서스 메커니즘이지만, 기존의 PBFT 컨센서스 메커니즘은 컨센서스 효율 측면에서 퍼블릭 체인의 요구를 충족시키지 못합니다. DREP은 Scenorr 멀티 시그니처 알고리즘을 사용하여 PBFT를 향상시켜 다수의 서명을 하나의 시그니처로 통합하고 스토리지 및 네트워크 전송에서 DREP 체인 효율성을 향상시키며 네트워크 전송 오버헤드를 줄입니다. 따라서 DREP 체인 시스템에 PBFT를 적용할 수 있습니다.

2.1.4 DREP developer tools

DREP은 Docker, IDE 및 기타 상위 수준 도구는 물론 콘솔 및 기타 기본 서비스를 비롯하여 DApp 개발 및 서브체인 사용자 지정 개발을 위한 일련의 개발 리소스를 제공합니다. 또한 DREP

개발자를 돕기 위해 browsers, faucets, testnets 등과 같은 테스트 도구가 만들어집니다.
DREP Docker는 빠른 설치, 쉬운 설치 및 배치의 장점을 가지고 있습니다. DREP 콘솔은 프로그래밍 및 대화 형 기능을 제공하며 스크립트 작업을 지원하며 개발자에게 유용합니다. RPC 인터페이스 및 JS 라이브러리는 노드 엑세스와 같은 여러 기능에 사용될 수도 있습니다.

2.2 Separated public chain ecosystem and small blockchain user base

블록체인의 가장 큰 경쟁은 "메인 체인"에 있습니다. 각 메인 체인은 블록체인 인프라의 대표 제품이 되기 위해 노력하며, 따라서 기술 분야에서 'Apple' 또는 '마이크로소프트'의 위치를 확보합니다. 결과적으로, 운영성 제한은 인프라에 따라 DApp에 따라 달라지며 ETH 및 EOS 사용자와 같이 사용자 기반이 분리됩니다. 이 때문에 퍼블릭 체인 개발에서 불가피하게 ' Prisoner's Dilemma'로 이어집니다.

DREP 기반 DREP ID는 다양한 퍼블릭 체인에 분산된 사용자 계정을 동화시키고 이 모델을 기존의 플랫폼으로 더욱 확장하여 더 많은 사용자가 블록체인에 마찰 없이 액세스할 수 있도록 하여 소규모 사용자 기반 문제를 해결함으로써 다양한 퍼블릭 체인 간의 장벽을 깨고 더 많은 사용자를 확보할 예정입니다.

2.2.1 DREP ID는 디지털 자산을 연결합니다.

DREP ID는 DREP 클라이언트를 통해 모든 유형의 암호화를 통합하여 사용자가 원스톱 계정 관리에 액세스할 수 있도록 합니다. 또한 서로 다른 플랫폼 주소를 DREP ID에 바인딩하면 크로스 체인 상호작동을 통해 크로스 플랫폼 전송이 가능합니다.

이 기능은 블록체인 애플리케이션 내에서뿐만 아니라 DREP ID를 통해 DREP와 협업하는 전통(중심화) 플랫폼 등과도 플랫폼 관리를 할 수 있으며, 기존 플랫폼의 수치 시스템, 포인트 시스템, 경제 시스템 등을 변경하지 않고 데이터와의 통합, 정보 암호화 보호 등과 같이 완전한 탈중심화 폐환 생태계를 형성합니다.

이러한 방식으로 DREP ID는 크로스 체인 Super DApp을 지원하여 DApp 개발자와 사용자가 인프라 제한 없이 메인스트림 통화를 자유롭게 전송할 수 있으며, 탈중앙화 거래소로 토큰을 자유롭게 거래할 수 있습니다. DApp의 사용자 환경을 개선하고 DApp 개발자가 사용자 범위를 확장하고 반복적인 개발을 줄이는 데 중요한 지원을 제공합니다.

2.2.2 DREP ID는 사용자 정보를 연결합니다.

블록체인의 진입 장벽과 사용법은 복잡한 20 자리 이상의 공개 키 주소에 있습니다. EOS와 같은

소수의 퍼블릭 체인만이 이 문제를 해결했습니다. 그럼에도 불구하고 EOS에 등록 된 각 주소는 여전히 지불해야 합니다. 더욱이 주소가 많으면 암기가 문제가 되어 가격이 급등합니다.

DREP 사용자는 이해할 수 있고 기억할 수 있는 별칭을 사용할 수 있습니다. 이렇게 하면 임계값을 블록체인 사용으로 낮출 수 있습니다. 또한 여러 주소를 한 이름으로 관리하면 가스 감소 및 DREP의 별칭이 20자리 이상의 퍼블릭 키 주소를 암기할 필요가 없으며, DREP은 이미 블록체인에 저장되어 있는 계정 닉네임만을 취급합니다.

기존 계정의 경우 DREP ID로 연결할 때 특정하고 복잡한 정보를 기록할 필요가 없습니다. DREP ID가 새 서브 계정을 생성한 후 주소 기록도 불필요해집니다. 이는 Alias가 사용자의 DREP ID 마커 역할을 하여 DREP Reputation Protocol을 통해 다양한 하위 계정을 연결함으로써 사용자의 신뢰도에 기여하고 사용자의 "제2의 ID" ——DREP ID에 대한 인식을 높여 주기 때문에 최종 사용자에게 편리합니다.

2.2.3 DREP ID는 사용자의 개인 정보를 보호합니다.

많은 중앙화 플랫폼이 사용자의 동의 없이 사용자의 데이터를 분석하고 재판매합니다. 어떤 사람들은 심지어 사용자들을 속여 관련 정보를 구매하기도 합니다. DREP ID를 사용하면 데이터를 공개 여부에 대해 사용자가 결정할 수 있습니다. 이용자의 프라이버시 면에서는 제3자가 비용을 지불해야 이런 개인정보를 수집할 수 있습니다. 그 결과, 사용자는 보상금으로 DREP 토큰을 받을 수 있으며, 제3자는 사용자의 평판 가치와 낮은 데이터 구입 비용과 같은 메트릭스를 포함하여 보다 정확한 데이터를 얻을 수 있습니다.

중앙화 플랫폼에 로그인할 때 서버는 사용자 이름, 사용자 계정 등과 같은 정보에 액세스할 수 있습니다. 사용자가 관련 계정으로 로그인할 때 플랫폼은 또한 사용자에게 알리지 않았음에도 불구하고 프로필을 작성할 수 있습니다. DREP ID는 타사 로깅과 결합되어 개인 정보 침해 방지를 위해 사용자에게 어떤 정보 플랫폼을 획득할 수 있는지, 어떤 방식으로 로그인할 수 있는지를 선택할 수 있는 권한을 부여합니다. 따라서 사용자는 개인 정보를 보호하면서 수많은 계정 및 암호를 기억할 필요가 없습니다.

2.3 블록체인 기술과 기업의 요구사항이 일치하지 않습니다.

블록체인은 프로덕션 혁신을 위한 방법으로 높은 기대를 받고 있습니다. 하지만 블록체인과 기업을 연결하는 데 한계가 있고 중앙화 서버보다 효율성이 낮으며 인재가 부족하기 때문에 이 분야의 발전은 더디기만 합니다.

DREP은 블록체인 개발자들이 "close the door" 시장 요구를 예측하는 것이 아니라, 시장을 보다 자세히 살펴보고 고객과 사용자의 실제 요구를 이해해야 한다고 생각합니다.

블록체인 개발의 고충점과 어려움을 학습한 후에는 쉽게 통합할 수 있는 키트를 여러 가지 다른 수직으로 개발할 수 있습니다.

시장 조사에 따라 DREP은 두 가지 솔루션을 제공합니다. 하나는 API 및 플러그인 지원을 위해 DREP 고급 기술 솔루션을 업그레이드하여 애플리케이션/엔터프라이즈 측면에서 블록체인 학습 비용, 개발 어려움 및 복잡성을 줄이는 것입니다. 다른 하나는 수직 도메인에 대한 맞춤형 SDK를 개발하여 개발의 특정 문제를 해결하고 완전한 수직 도메인 기술 솔루션을 구축하는 것입니다.

2.3.1 DREP API 및 플러그인을 사용하면 더욱 간편하고 쉽게 사용할 수 있습니다.

DREP API는 다양한 언어에 적응하기 때문에 중앙 플랫폼이 분산되기 쉽습니다.
DREP 플러그인은 보다 정확하고 복잡한 요구를 충족시키는 것을 목표로 하며 수직 도메인 개발에 도움이 됩니다.

DREP API 및 플러그인의 장점은 다음과 같습니다.
- 블록체인에 대한 완전한 이해가 없어도 Highly-targeted이 된 개발로 기능을 더욱 풍부하게 활용할 수 있습니다.
- 공동 개발을 지원하고 개발 프로세스 중에 조정 또는 수정을 용이하게 합니다.
- 실제 문제를 블록체인 솔루션으로 직접 변환하여 보다 쉽게 사용할 수 있습니다.

2.3.2 DREP SDK, aimed at vertical industries

DREP SDK는 모든 종류의 DApp을 지원합니다. DEP SDK를 통해 DApp R&D 팀은 원클릭으로 멀티 퍼블릭 체인 자산 버전, 내장 지갑 및 자산 거래 플랫폼을 출시할 수 있습니다. 또한 DREP ID를 기반으로 DApp R&D 팀은 더 많은 퍼블릭 체인 사용자를 획득하여 다양한 디지털 자산 소유자를 애플리케이션 사용자로 전환하고 Super DApp을 생성할 수 있습니다.

슈퍼 DApps: DApp은 특정 퍼블릭 체인에 국한되지 않고 다양한 디지털 자산을 연결하여 모든 사용자가 다른 경제 활동을 지불, 이전, 대여 및 수행할 수 있도록 합니다. 이와 동시에 기존 플랫폼 사용자는 블록체인 DApp 버전에 지원할 수 있어 사용자 교육 비용을 크게 절감할 수 있습니다.

블록체인 게임용 DREP SDK는 다음을 포함하며 이에 국한되지 않습니다.
- 게임 계정: 크로스 체인 DREP ID를 강조하여 현재 분리되어 있는 사용자 기반을 제거합니다;
- 결제 및 거래: 내장된 결제 및 거래 엔진을 강조하여 디지털 자산 교환 경험을 개선합니다.
- 디지털 운영: 게임 운영에서 데이터 시각화, 투명성 및 구성 가능성을 강조합니다.

DREP 기술 프레임워크

3.1 DREP 퍼브릭 체인

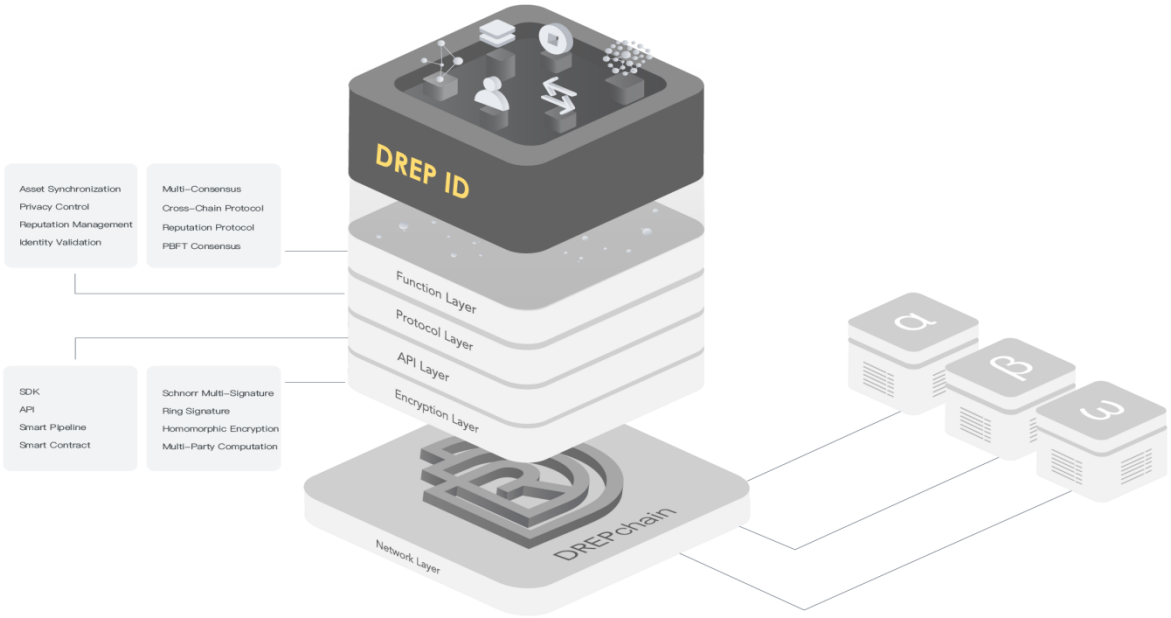
DREP 체인은 DREP 팀에서 완전히 개발 한 고성능 퍼블릭 체인으로서 EVM 및 WASM 형식의 스마트 계약과 호환을 가능하며 루트 체인 및 서브 체인으로 구성된 dual-layer 구조입니다.

루트 체인은 주로 서브 체인 및 DREP 토큰 트랜잭션에 대한 데이터 동기화를 담당하며, 서브 체인은 기업에서 DApp 및 자체 블록체인 에코 시스템을 보다 쉽게 개발할 수 있도록 합니다. 이를 통해 기업은 토큰을 독립적으로 배포하고, 스마트 계약 및 스마트 파이프라인을 배포하고, 자산을 거래하고, 멀티 체인에서 평판 가치를 공유 할 수 있습니다.

DREP Chain은 컨센서스 선택과 관련하여 효율성을 우선시합니다. 이것은 DREP Testnet 1.0에서 개선 된 PBFT가 서브 및 루트 체인에 대한 공통 메커니즘으로 배포 된 이유를 설명합니다. 미래에는 루트 체인이 점차 POS 시스템을 채택하여 평판을 얻습니다.

전통적인 PBFT 합의 메커니즘에서 발전한 DREP은 multi-party signature을 기반으로 하는 PBFT를 도입하여 TPS뿐 아니라 저장소 및 네트워크 전송 프로세스에서도 효율성을 향상시킵니다. 원래의 PBFT 프로토콜을 사용하여 참가자는 정보 서명을 리더에게 보내야 했고 리더는 블록 헤더에 서명을 통합했습니다. 멀티 서명을 사용하면 블록 헤더의 크기를 늘릴 수 있습니다. DREP은 Secv256k1 타원 곡선이 지원하는 Schnorr multi-party signature 알고리즘을 배포하여 하나의 서명 만 생성하므로 서명 길이가 크게 줄어들어 블록 헤더의 크기와 저장 및 네트워크 전송 비용이 크게 줄어 듭니다.

DREP 기술 구조는 다음과 같습니다.

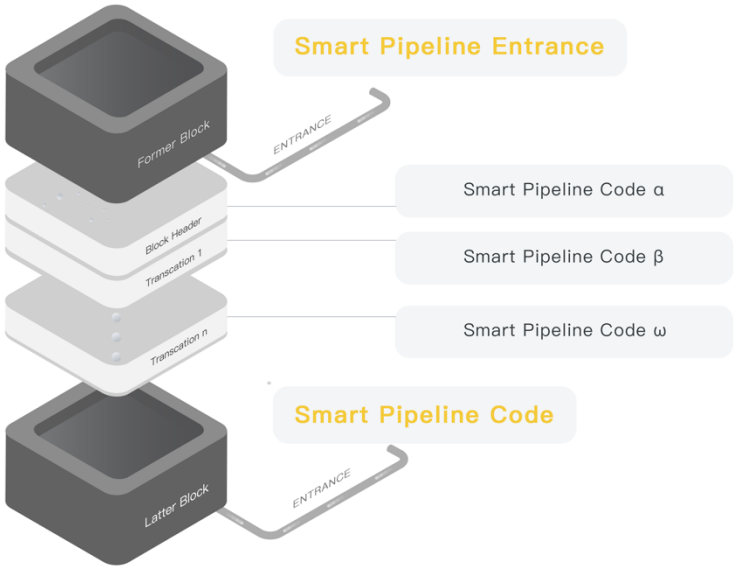


3.1.1 DREP Smart Pipeline

DREP은 블록 처리 가상 컴퓨터와 외부 응용 프로그램간에 데이터 처리 및 데이터 전송을 향상시키기 위한 스마트 파이프라인 개념을 제안합니다. 스마트 파이프라인은 Ethereum과 같은 플랫폼에서 이미 널리 사용되는 스마트 계약과 비교할 때 고효율, 강력한 확장 성 및 제로 가스 소비라는 이점을 자랑합니다.

스마트 계약의 문제점은 다음과 같습니다.

• 블록 패키지에는 최대 데이터 용량이 매우 제한되어 있습니다. 예를 들어, ETH 모델, 단일 블록의 현재 최대 가스는 3,141,592 가스입니다. 이는 첨부된 데이터가 1M에 도달하지 못하면 용지 걸림이 발생할 수 있음을 의미합니다. 즉, DApps는 막힘에 대한 두려움 때문에 많은 양의 데이터에 대처할 수 없다는 것을 의미합니다.
• 스마트 계약서를 읽고 쓰고 계산하는 비용은 엄청납니다. 결과적으로 개발자는 전통적인 플랫폼에서 널리 사용되는 알고리즘을 사용하는 것을 꺼려하지만 블록체인에서 대량의 가스를 소비하여 DApp 디자인을 제한합니다.
• 활성 통화 기능이 없으므로 스마트 계약이 외부 스크립트 지원이 필요한 고정 시간 작업과 같은 복잡한 작업을 자동으로 수행할 수 없습니다.
스마트 파이프라인의 스케치는 아래와 같습니다:



블록체인에서 블록이 생성되면 가상 시스템에서 트랜잭션이 차례로 수행됩니다. 스마트 파이프라인은 각 실행 전후에 삽입할 수 있습니다. 스마트 파이프라인은 브레이크포인트 역할을 하며 클라이언트는 필요에 따라 파이프라인/브레이크포인트의 일부를 활성화할 수 있습니다. 클라이언트가 활성화된 스마트 파이프라인/Breakpoint를 실행하면 정지 작업 프로세스가 자동으로 트리거되고 스마트 파이프라인을 통해 외부 애플리케이션으로 실시간 데이터가 전송됩니다. 외부 응용 프로그램은 데이터 처리를 담당하며, 처리 후 결과는 스마트 파이프라인을 통해 블록체인 상의 클라이언트로 전송됩니다. 여기서 클라이언트는 데이터를 데이터베이스에 저장하여 블록체인 데이터 업링크를 완료합니다. 이러한 프로세스는 가상 시스템에서 대량의 데이터 처리 문제를 방지합니다. 전송은 작동 효율을 저해하지 않으며, 대신 DREP에 의해 스마트 파이프라인이 깊이 최적화되어 있기 때문에 데이터 처리를 개선합니다.

DREP 스마트 파이프라인 애플리케이션은 블록체인 전체에 배포되는 WASM 명령 집합으로 구성됩니다. 또한 서브 체인에 따라 자체 작성 및 검증된 응용 프로그램에서 실행하거나 실행할 다른 응용 프로그램을 선택할 수도 있습니다.

3.1.2 DREP cross-chain protocol

DREP 크로스 체인 프로토콜은 평판과 같은 개인ID(신용 등급 / 신뢰성)와 관련된 행동 데이터를 동기화 및 마이그레이션 한 후 자산을 전송하기 위한 크로스 체인 트랜잭션에 대한 전통적인 사고를 초월하고 동형 암호화를 통해 보안을 유지합니다.

DREP은 서로 다른 요구를 충족하고 서로 다른 구조 내에서 성능과 비용 균형에 대처하기 위해 동형 및 이형 크로스 체인 솔루션을 모두 채택합니다.

- **Isomorphic cross-chain:** DREP 메인 체인과 서브 체인은 마찰 없는 동형 크로스 체인 프로토콜로 연결됩니다. 이를 통해 사용자는 지갑을 통해 크로스 체인 플랫폼 간의 실시간 변화를 볼 수 있습니다.
- **Heterogeneous cross-chain:** 분산형 개인 키 제어 기술은 DREP 시스템 외부의 체인을 DREP 에코시스템에 연결하여 안전한 이형 크로스 체인을 달성함으로써 여러 플랫폼에 대한 평판 프로토콜을 확장합니다.

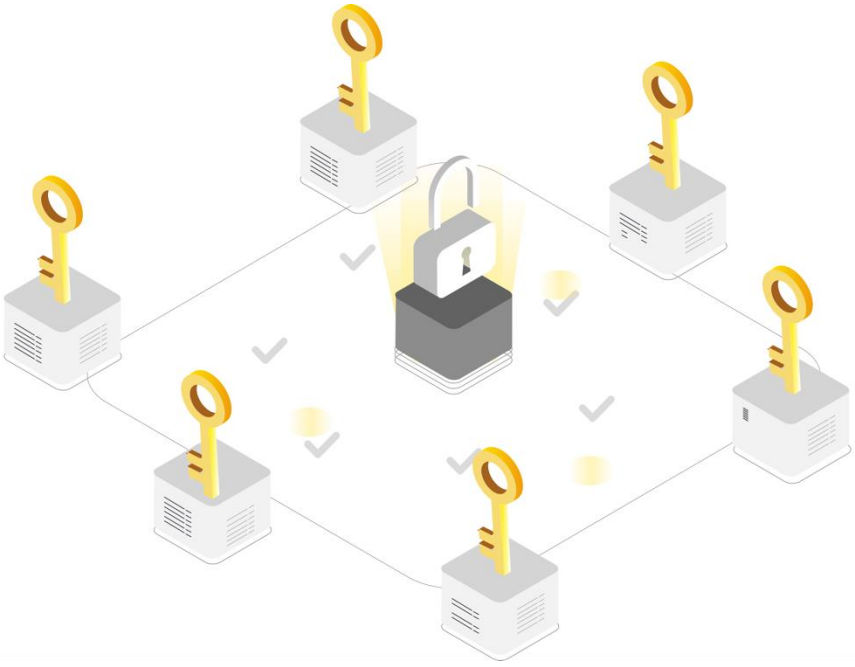
동형 및 이형 크로스 체인 기술을 기반으로 하며, 다양한 DApp의 토큰 자산 및 평판 데이터가 메인 계정에 통합되어 다단계적이고 생생한 사용자 평판 프로파일을 형성합니다.

또한, DREP은 파트너의 사용자 행동을 "재평가"하여 크로스 도메인 보안 제어 요구사항에 따라 다른 시스템으로 평판을 확장하고 블록체인을 넘어 평판을 가능하게 함으로써 광범위한 평판 생태계를 형성할 계획입니다.

Distributed private key control

분산형 개인 키 제어는 탈중앙화 기술을 사용하여 여러 개인 키를 사용하여 크로스 체인 자산을 제어합니다. 원래 소유자는 여전히 소유권이 있지만 개인 키 한 개로는 자산을 인출할 수 없습니다. 보유자가 자산을 인출하려면 해당 체인을 신청하고 충분한 개인 키를 확보해야 합니다.

예를 들어, 사용자 Alice는 한 토큰을 한 체인의 토큰에서 다른 체인으로 변환하려고 합니다. 체인에 걸친 다수의 노드(shards/super-compactive Committee)는 원래 체인에 하나의 멀티 서명된 계정을 유지하고, 개인 키를 할당한 다음 별도로 제어하여 단일 노드가 충분한 개인 키 없이 원래 체인의 토큰을 가져올 수 없도록 합니다.



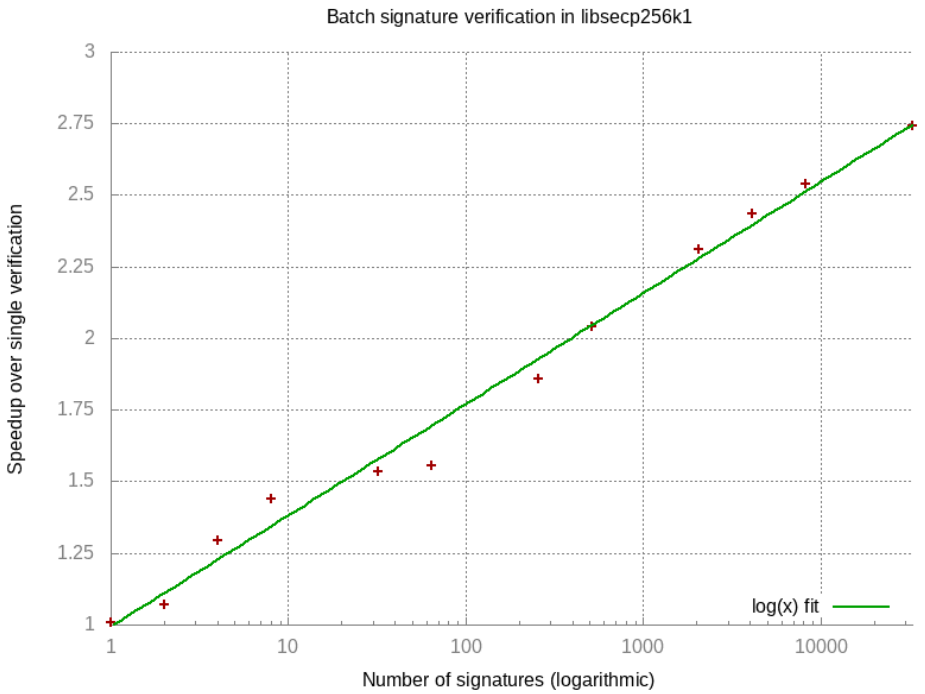
Alice가 하나의 토큰을 DREP에 의해 제어되는 멀티 서명 계정에 보관할 때, Alice는 DREP의 한 토큰은 동기적으로 릴리스된 예금 토큰과 동일하며, 다른 체인의 토큰을 통해 DREP의 다른 노드와 교환할 수 있습니다. Alice가 원래 체인에 있는 토큰 한 개의 소유권을 취소하고 싶을 때, DREP에 남아 있는 토큰을 잠그고 나서 원래 체인에 있던 토큰과 동일한 양의 토큰을 풀어 주어야 합니다.

분산된 개인 키 제어 프로세스는 보다 안전하며, multi-currency complex 계약을 포함한 스마트 계약을 지원합니다. 이는 원래 체인이 스마트 계약을 지원하는지 여부와 관계없이 체인에 토큰을 배포하는 경우에 해당합니다.

3.1.3 DREP 개인 정보 보호입니다.

Schnorr multi-party signature

DREP은 멀티 파티 서명을 기반으로 하는 PBFT 메커니즘을 도입합니다. 기존 PBFT 프로토콜에서는 참가자가 리더에게 정보 서명을 전송한 다음 리더가 서명을 블록 헤더에 통합해야 합니다. 그러나 여러 개의 서명이 있을 경우 블록 헤더의 크기가 증가하여 네트워크 전송 효율성에 영향을 미칩니다. DREP은 Secp256k1 타원곡선에 기반하여 Schnorr 멀티파티 시그니처 알고리즘을 배포하므로 블록체인 효율성이 크게 향상됩니다.
BIP-Sechnorr 서명의 Sthnorr 멀티 파티 서명 성능 테스트 결과는 다음과 같습니다.



다른 서명 양식과 다른 Schnorr 다중 파티 서명은 결국 하나의 서명만 생성합니다. 이렇게 하면 서명 길이와 블록 헤더 크기가 크게 줄어들어 스토리지 및 네트워크 전송 비용이 절감됩니다.

또한 향후 개인 정보 트랜잭션을 강화해야 하는 경우, 멀티 파티 서명이 개인 정보 보호에도

도움이 됩니다.

동형 암호화 및 개인 정보 보호입니다.
DREP 체인 작업 과정에서는 내부 스마트 파이프라인이나 외부 데이터 공유와 같은 정보를 제3자에게 전달하는 것이 불가피하며, 이 과정에서 사용자 개인 정보 유출이 발생하여 사용자 ID 보안이 위험해질 수 있습니다. 이를 위해 DREP은 사용자가 이 개인 정보를 처리할 때 데이터 프라이버시를 보호하기 위해 동형 암호화를 채택합니다.

알고리즘은 2차 정수 그룹의 n번째 잔차 클래스를 계산하는 암호화 문제를 기반으로 Paillier 기법을 사용합니다.

여기서 m은 암호화된 메시지와 $m\in(0,n)$를 의미합니다. 그런 다음 생성된 key pairing을 통해 임의 r0,(0,n)를 선택합니다. 퍼블릭 키(n,g)와 개인 키(λ,u), 암호 텍스트 C를 $C=g^m r^n \mathrm{mod} n^2$로 계산합니다.

Ciphertext C는 동형 및 동형 혼합 곱셈 평문입니다.

- **Homomorphic addition of plaintexts**

  $D(E(m_1,r_1)E(m_2,r_2) \bmod n^2)=m_1+m_2 \bmod n$

  $D(E(m_1,r_1)g^{m2} \bmod n^2)=m_1+m_2 \bmod n$

- **Homomorphic mixed multiplication of plaintexts**

  $D(E(m_1,r_1)^{m2} \bmod n^2)=m_1m_2 \bmod n$

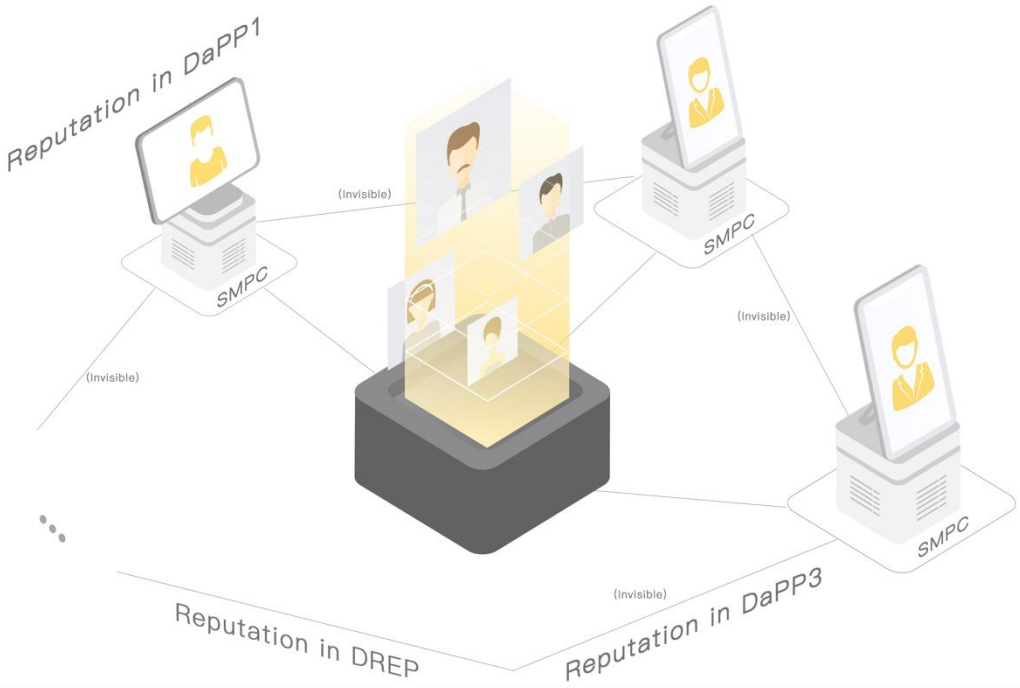
따라서 암호화 후 다양한 데이터 처리를 수행할 수 있으며, 그 결과를 사용자에게 다시 보낼 수 있습니다. 사용자는 개인 키를 통해 일반 텍스트 데이터 처리에 의해 수행된 동일한 결과를 얻을 수 있으므로 데이터 누설이 불가능합니다.

위의 내용과는 별도로 동형 암호화 시그니처를 컨텐츠에 추가할 때 데이터 처리 중 오식 처리, 스푸핑 및 기타 형태의 부정행위를 확인하여 데이터 정확성을 보장할 수 있습니다.

Secure multi-party computation
개인 키를 공유하는 여러 사람이 참여하는 분산형 개인 키 제어 및 링 서명이 진행되는 과정에서 모든 민감한 정보를 완전히 노출하지 않는다는 원칙을 따를 필요가 있습니다. 따라서 DREP은 데이터 보안을 보호하기 위해 시큐어 멀티 파티 연산을 선택합니다. 전체 정보는 사용 중인 경우에만 사용할 수 있습니다.
시큐어 멀티 파티 계산은 다음과 같은 문제를 해결합니다. n 개인은 각각 개인 정보 보호 x1, x2, ... xn을 사용하여 특정 함수 y = f(x1, x2, ... xn)를 계산하지만 이러한 개인은 다른 개인의 개인 정보에 액세스할 수 없습니다. 실제 세계에는 다른 사람의 개인 정보를 얻으려는 악의적인

노드가 있습니다. 시큐어 멀티 파티 계산 프로토콜은 모든 참가자가 악의적인 의도를 가지고 있는지 여부와 상관없이 출력을 넘어서는 추가 정보에 액세스할 수 있는 권리를 거부합니다.

DREP은 평판 계산을 예로 들며 동형 암호화, 방탄 및 기타 조치를 통해 시큐어 멀티 파티 계산을 수행합니다.



DREP은 시큐어 멀티 파티 연산을 구축하여 각 DApp 및 DREP 플랫폼 내에서 중요한 데이터를 암호화합니다. 거래 중 데이터 전송이 유출되더라도 사용자의 원래 데이터는 안전합니다. 시큐어 멀티 파티 계산은 또한 데이터 전송과 관련된 두 당사자가 안전한 방법으로 데이터를 암호화 및 해독할 수 있도록 보장합니다. 이와 동시에 각 DREP DApp에 있는 사용자의 공용 키, 주소 및 데이터는 독립적이며 보이지 않습니다.

3.1.4 개선 및 최적화를 지원합니다.

DREP가 DREP 체인을 개발하는 중요한 이유 중 하나는 기존 블록체인 메인체인과의 강력한 결합으로 인해 현재 기존 엔터프라이즈 시스템과의 원활한 통합에는 적합하지 않습니다. 또한 많은 High-TPS 메인체인이 높은 동시 요청을 전송하기 위한 기존 성능 요구 사항을 충족하지 못합니다.

구조 최적화는 다음과 같습니다.

DREP은 데이터베이스, 네트워크 및 컨센서스의 다양한 부분을 모듈화한 다음 이를 컨테이너에 별도로 저장합니다. 미들웨어를 통해 모듈식 호출을 수행하여 각 모듈의 솔루션을 제공합니다. 또한 인프라에서는 미들웨어를 통해 컨테이너 등록, 활성화 및 업그레이드와 같은 일련의 작업을 자동으로 구현할 수 있습니다. 서브 체인 개발자의 경우, DREP 체인 인프라 코드는 명확한 논리와 쉬운 재구성을 자랑합니다. 또한, DREP은 라우팅 및 메시지 배포 메커니즘을 사전에 구축하여 네트워크와 합의 계층을 완전히 분리함으로써 적용 가능한 합의 범위를 PBFT 이상으로 확장함으로써 하위 체인 독립 개발 합의를 용이하게 합니다.

가상 시스템 최적화는 다음과 같습니다.

또한 DREP은 DREP 체인 비즈니스 요구사항을 충족하기 위해 기존 EVM을 개선했습니다.
- 서로 다른 체인에서 스마트 계약 집행을 실현합니다.
- DREP 비즈니스에 따라 평판 관련 주문이 증가합니다.
- 각 서브 체인에서 자동 구성 및 수요 조정을 가능하게 하여 가스 가격을 업그레이드합니다.
- 비즈니스 요구에 따라 인프라 데이터베이스를 다시 설계합니다.

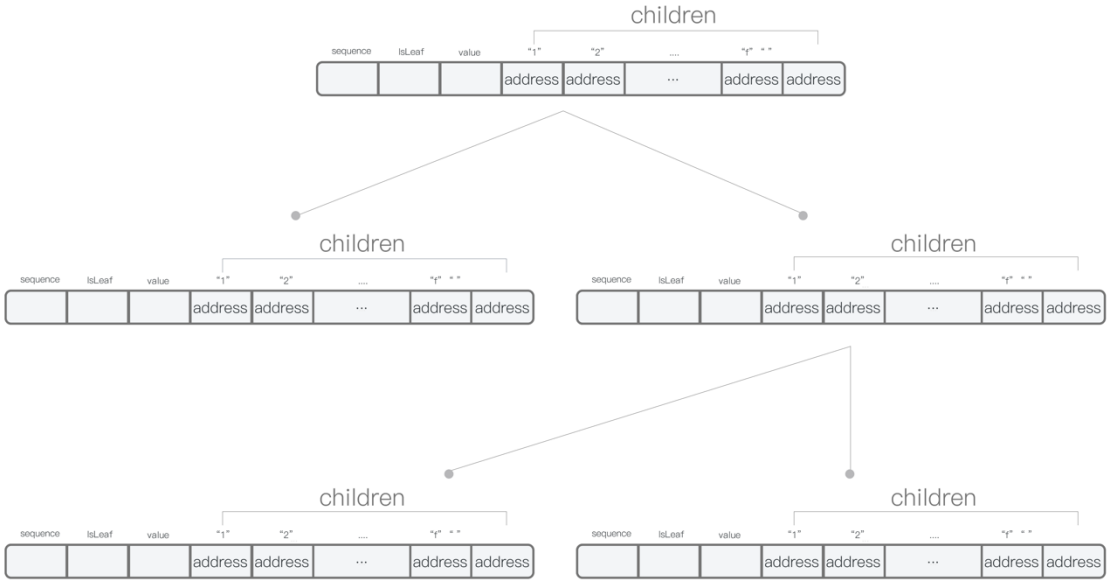
서브체인 기능이 향상되었습니다.

서브체인 데이터를 메인 체인에 동기화하는 과정에서 서브 체인 데이터 오류가 발생할 경우 롤백이 필요하며, 원래 레벨 DB가 이를 지원하지 못합니다. 또는 자체 개발한 서브 체인 보금자리 및 롤백으로 지원되는 DREP가 이러한 문제를 해결할 수 있습니다.

데이터베이스 최적화입니다.

동시 요청이 많을 경우 캐싱 메커니즘이 큰 압력을 받게 됩니다. 즉, '높은 TPS'가 반드시 높은 트랜잭션 볼륨과 같은 것은 아닙니다. 또한 DREP은 캐시, 데이터베이스 등을 최적화 및 개선하고, LRU 캐쉬 내에서의 정밀 잠금 기능을 사용하여 TPS 5000에 도달해도 고성능을 보장합니다.
DREP 체인 레벨 DB 데이터베이스는 Hash Patricia Tri(Hitton Prefix Tree, 여기서 HPT라고 함) 기술을 활용하여 사용자의 계정 상태 변화를 보존합니다.

HPT는 K-트리 데이터 구조이며, 트리의 각 노드는 다음 4가지 속성으로 구성됩니다. Sequence, Value, Children 및 IsLeaf4입니다. HPT 루트 노드의 값 속성은 블록 확인을 위해 현재 데이터베이스의 해시 값을 보존하므로 시퀀싱 속성이 특정 전체 키를 가져올 수 있는 유일한 방법입니다.



사용자 계정이 변경되면 데이터베이스가 변경 내용을 반영하여 HPT를 변경하게 됩니다. 사용자 계정의 16진수 문자열 키를 기준으로 데이터베이스는 특정 리프 노드를 찾을 때까지 루트 노드에서 시작하여 전체 키를 얻기 위해 검색 경로의 모든 Sequence 속성이 통합됩니다.

HPT의 두 가지 주요 이점은 다음과 같습니다.

o 첫째, 트리 구조와 해시 알고리즘의 불가해성과 극단적으로 낮은 충돌 특성은 데이터베이스 설명의 편리성과 신뢰성을 향상시킵니다.
o 둘째, 데이터베이스의 핵심 가치 설계와 접두사 트리의 데이터 압축은 쿼리 및 수정의 효율성을 크게 향상시키고 계산 비용을 절감합니다. 각 계정 수정 후 HPT 깊이 수와 동일한 트리 노드 작업을 통해 데이터베이스 업데이트를 완료할 수 있습니다. 한 트랜잭션에서 수정 내용이 여러 개일 경우 MPT 수정에서 발생하는 계산 증가가 필요한 계정 정보 양에 훨씬 못 미칩니다. 더 많은 계정 정보를 사용하면 더 많은 MPT 계산을 절감할 수 있습니다.

계정 정보를 보존하기 위해 Ethereum이 사용하는 프레픽스 트리 구조와 비교하여 DREP HPT는 트리 노드를 통일하고 최적화합니다. Ethereum의 null노드, 리프노드, 확장 노드 및 분기 노드를 채용하는 대신 DREP HPT를 사용하면 프레픽스 트리의 높이와 검색 시간이 단축되어 HPT 쿼리 및 수정의 성능을 향상시킵니다.

3.2 DREP ID

DREP ID는 DREP 및 협업 응용 프로그램 플랫폼에서 사용되는 디지털 ID뿐만 아니라 사용자 자산의 입구 포털입니다. 여기에는 해당 플랫폼에서 사용자가 생성 한 디지털 이미지의 합계가 포함됩니다.

B측 고객의 경우 DREP ID는 사용자 트래픽 및 고품질 데이터의 입구 포털이며 멀티 통화 / 암호화폐로 지불 할 수 있는 크로스 체인 자산 상호 작용의 단축키입니다.

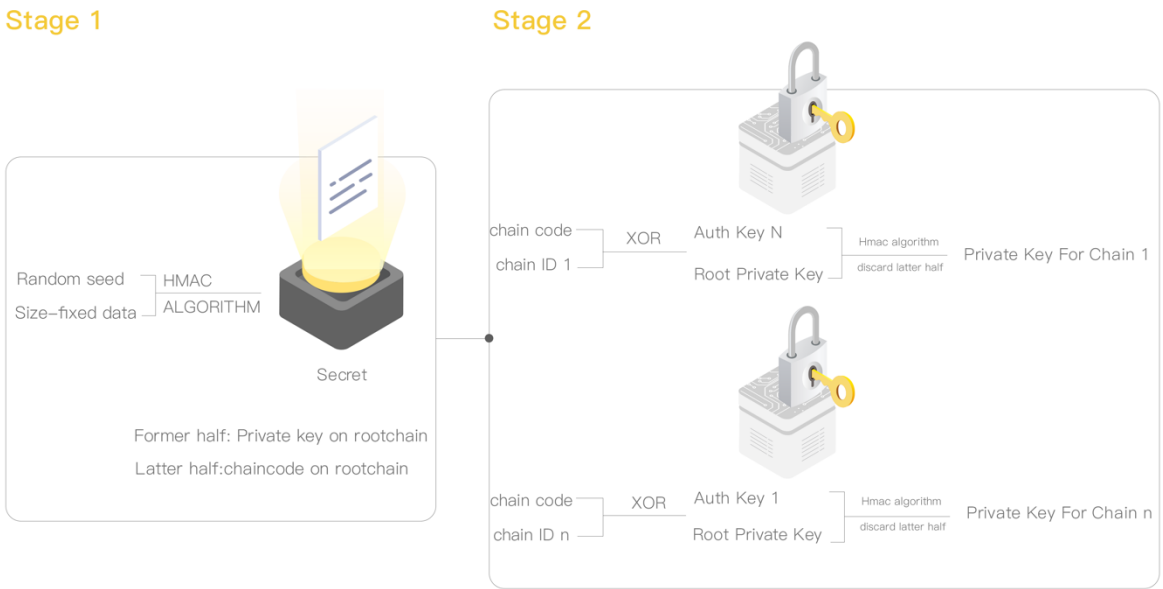
3.2.1 보안성

DREP 에코시스템을 사용할 때 모든 사용자는 마스터 계정과 여러 개의 서브 계정을 가집니다. DREP ID는 여러 애플리케이션에 걸쳐 평판 데이터와 자산을 연결하고 전체 사용자 평판 프로필 이미지를 구축하는 연결 역할을 합니다.

DREP은 HMAC(Hash Message Authentication Code) 알고리즘을 기반으로 마스터 계정을 사용하여 서브 계정을 생성합니다.

HMAC의 공식은 다음과 같습니다.

$$HMAC(K,m) = H\Big((K' \oplus opad) \mid\mid H\big((K' \oplus ipad) \mid\mid m\big)\Big)$$



K는 마스터 계정 키이고, m은 서브 체인 ID이며, opad와 ipad는 모두 특정 상수입니다. 각 서브계정의 개인 키는 마스터 계정의 개인 키와 해당 서브 체인 ID에 의해 생성되며, 이를 통해

마스터 계정은 각 응용 프로그램에서 서브 계정을 제어할 수 있습니다. 이는 안정성을 가진 이유는 다음과 같습니다.

- Master key control: 사용자가 서브 체인 계정의 개인 키를 생성하고 획득할 때 해당 마스터 계정의 개인 키, 확인 코드 및 서브 체인 ID도 필요합니다. 따라서 서브 체인 계정의 개인 키 보안이 보장됩니다.
- Unconnectable: 비대칭 암호화 보호 하에서 메인 또는 서브 체인에 관계없이 계정을 역방향으로 연결할 수 없으므로 정보를 익명 온-체인으로 만듭니다.

DREP HMAC는 BTC HD 지갑과 비교하여 다음과 같은 이점을 제공합니다.

- Variable address length and higher security:

DREP은 SHA3 SHAKE256(SHAKE=SHA+kecak)을 사용하여 퍼블릭 키를 해시하므로 출력 주소를 설정하여 더 높은 성능과 보안을 달성할 수 있습니다.

- 계산 비용 절감:

HD 지갑은 서브 계정 주소를 찾기 위해 많은 수의 서브 개인 키가 필요합니다. DREP에서는 마스터 계정 주소를 서브 계정의 주소와 연결하여 저장소 및 계산 비용을 절감하는 Private Seed로 인해 서브 개인 키가 선택 사항입니다.

또한 DREP은 사용자 ID 정보를 보호하기 위해 시큐어 멀티 파티 계산, 링 서명 및 기타 조치를 채택하여 데이터 남용 및 누출 위험을 최소화합니다.

3.2.2 Zooko Triangle breakthrough

DREP ID의 별칭 ID 시스템은 Zooko 삼각형을 지정합니다. 사용자는 안전하고 탈중앙화 환경에서 ID의 표현으로 이해할 수 있는 별칭/닉네임을 생성하므로 쉽게 기억할 수 있고 명성과 프로필 이미지에 도움이 됩니다.

3.2.3 Universality

DREP ID는 DREP SDK를 통해 탈중앙 로깅을 달성합니다. 한편, DREP ID는 타사 로깅과 자체 소거 ID의 장점을 가지고 있는 반면, DREP ID를 사용하여 로그인할 수 있는 많은 애플리케이션을 지원하며 전송된 정보를 제어합니다. 또한 DREP ID는 BTC, ETH, EOS 및 기타 블록체인 구조와 호환되며, 애플리케이션 위치와 같은 블록체인 제한을 초월합니다.

3.2.4 Convenience

DREP ID는 여러 자산을 연결하여 자산 장벽을 해소하고 체인 간 전송을 용이하게 합니다. DREP Client는 다양한 다른 애플리케이션 및 플랫폼에 통합되어 다중 자산 결제 및 거래를 지원합니다.

사용자가 DREP ID를 사용하여 ID 데이터를 저장한 후에는 정보가 자동으로 선택되어 필요할 때 애플리케이션에 전달됩니다.

3.2.5 Uniqueness

DREP ID는 사용자 등록을 제한하지 않으며 분산으로 인해 사용자가 KYC를 수행하도록 강제하지 않습니다. ID 평판 이미지가 풍부해지면 사용자에게 큰 혜택을 줄 수 있다는 점은 인정됩니다. 따라서, 여러 개의 분산된 ID보다는 하나의 고유한 ID를 사용하는 것이 더 신뢰되기 때문에, 서브 계정 형태의 다른 애플리케이션 계정을 DREP ID에 바인딩하는 것은 사용자의 신뢰성과 평판에 도움이 됩니다. 그 결과, 사용자들은 "제2의 identity"를 생성하려는 동기를 갖게 될 것입니다.

3.3 DREP 평판 프로토콜

DREP 평판 시스템은 DREP ID 시스템과 함께 장기적인 가치를 지닌 ID를 부여하여 고객/사용자 충성도 향상, 진정한 가치 있는 포인트 시스템 만들기, 온라인 신용 점수 획득, 정확한 사용자 프로필 이미지 및 고품질 사용자 획득과 같은 문제를 해결하여 B2B2C 제품을 크게 지원합니다.

3.3.1 평판 시스템의 개요

DREP 평판 시스템에는 일반 평판 프로토콜, 평판 파이프라인 인터페이스, 체인 및 알고리즘 라이브러리로 업링크되는 평판, 평판 보상 취득, 평판 가치 계정 관리 및 허위 계정 식별 메커니즘 등이 포함되며, 이는 사용자의 행동을 명성과 연계시키는 환경 연결 구성입니다. uct 실시간 평판 정산 및 종합적인 다방간 평판 평가에 기반하여 사용자에게 피드백을 제공합니다.

일반 평판 프로토콜

- 다양한 플랫폼에서 블록체인까지 사용자의 평판 데이터와 데이터 변경 사항을 기록하여 변경할 수 없는 온체인 평판 모델링을 달성할 수 있습니다.
- 기존 장벽을 깨고 사용자의 행동 데이터를 크로스 체인으로 전송하여 실시간 평판 데이터 동기화를 형성합니다.
- 다양한 플랫폼 간의 사용자 평판을 사용자의 DREP ID에 통합하여 완전한 사용자 평판 프로필 이미지를 구축합니다.

평판 파이프라인

평판 파이프라인은 과도한 스마트 계약의 소비를 방지하기 위해 스마트 파이프라인을 채택하고 블록체인 성능에 영향을 주지 않고 데이터 처리를 개선하여 실시간 사용자 평판 정산을 실현합니다.

평판 알고리즘 라이브러리

DAPP는 다양한 산업에 적합하며 기능 및 소싱은 모두 매우 다릅니다. 따라서 단일 알고리즘으로 평판 값을 계산하는 것은 불가능하고 비과학적입니다. DREP 시스템에서 기본 평판 알고리즘은 시간에 따른 과거의 증가/감소 + 현재 값의 합계이며, DAPP에 대한 평판 값 계산 알고리즘이 제공되어 사업 모델 및 요구에 따라 맞춤형 설계를 할 수 있게 된다. 한편, DREP 시스템은 몇 가지 주요 산업 유형을 위해 설계된 알고리즘 템플릿을 생성하고 DAPP에 다음과 같은 옵션을 제공합니다.

- E-commerce
- Online Q&A
- Blog
- Forum
- Entertainment (video, music, game, etc.)

또한, DREP은 개발자 및 DAPP가 자체 알고리즘을 개발하고 오픈 소스로 만들도록 권장하기 위한 시도로 타사 알고리즘 라이브러리를 개발합니다. 또한 DREP은 플랫폼에 가입하는 타사 알고리즘 라이브러리에 대한 경제적 인센티브를 제공합니다.

평판 메커니즘

DREP의 핵심 개념은 평판을 부를 재현하고 그 가치를 발산하는 것입니다. 그렇기 때문에 DREP가 평판을 기반으로 인센티브 모듈을 만들고 설계한 이유입니다. 이 인센티브는 다양한 방법, 링크 및 관련 플랫폼 설계에 따라 사용자 동작을 계산하여 DREP에 의해 보상됩니다.

평판가치 계정 관리 및 허위 계정 식별 메커니즘

DREP의 평판 시스템은 모든 DAPP 플랫폼에 연결하여 모든 사용자를 평판 가치로 연결합니다. DREP은 에코시스템 사용자를 위해 엄격한 평판 가치 계정 관리를 유지합니다.

• 사용자는 각 DAPP 내에서 블록체인에 저장될 하나의 퍼블릭 키 주소에만 평판 값을 누적할 수 있습니다.
• DREP은 사용자 정의 서비스 또는 맞춤형 경제적 인센티브를 제공하기 위해 사용자를 분류, 필터링 및 승인하는 모든 DAPP를 지원합니다.
• 개인 정보 관리: 사용자는 자신의 평판을 관리하고 다른 DAPP에서 자신의 평판 가치에 액세스할 수 있는 플랫폼을 인증할지 여부와 자신의 개인 평판 가치를 다른 사용자가 볼 수 있는지 여부를 선택할 권리가 있습니다.

허위 계정은 DREP의 지속적인 연구 및 개선의 모듈로 식별됩니다. 인터넷 플랫폼의 변화와 사물의 인터넷과 기타 인터넷 기술의 결합으로 인해 허위 계정 감식 메커니즘이 개선되어야 합니다.

DREP은 평판 가치 인식 임계 값, Sybil 공격방지 메커니즘 및 타사 KYC (신원 정보 검증) 플랫폼을 통해 허위 계정을 제외하므로 사용자가 평판과 이미지를 자연스럽게 유지할 수 있습니다.

3.3.2 평판 시스템의 장점입니다.

Universality

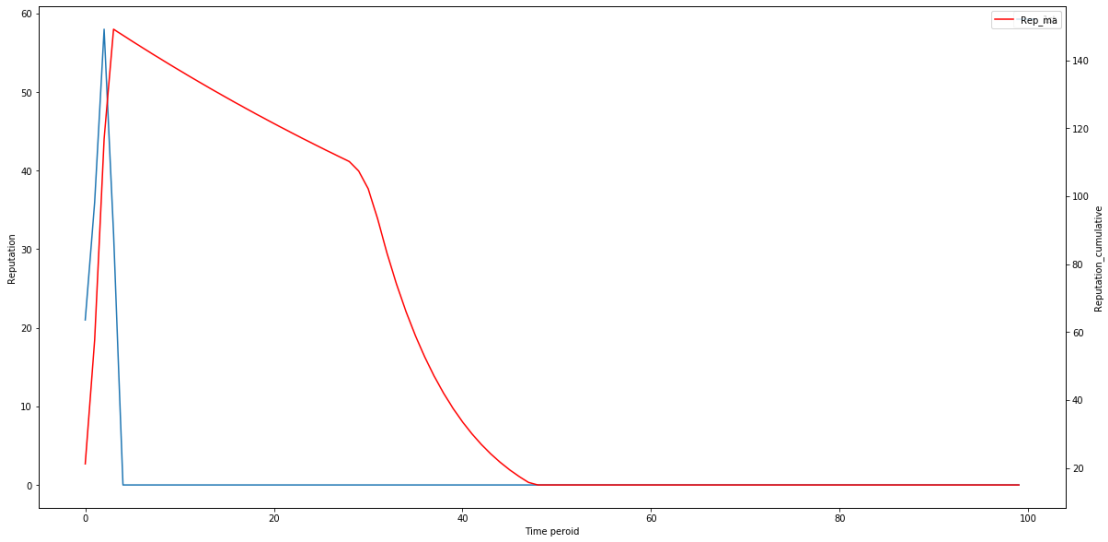
평판 프로토콜은 특정 플랫폼에 맞게 설계되지 않고 크로스 플랫폼과 데이터 통합을 특징으로 하는 서로 다른 템플릿을 사용하는 업종에 적합합니다. 업계/플랫폼이 작은 조정을 통해 사용자의 충성도를 얻는 것이 더 쉽습니다. 또한 사용자가 원하는 대로 데이터를 공유할 수 있으므로 데이터 수집 비용이 절감됩니다.

Time-effectiveness

DREP 평판은 사용자 행동 측면에서 시간 효율적입니다. 즉, 오래 전에 어떤 일이 발생할수록 평판에 미치는 영향이 줄어들어 DAU가 활성화되고 사용자의 플랫폼 의존도가 높아집니다.

평판 파이프라인을 통한 평판 시간 효율성은 사용자 평판의 일상적 또는 즉각적인 변화에 반영됩니다.

평판 시간 효과의 계산은 DREP 개발 팀이 제안한 평판 붕괴 획득 모델을 기반으로 합니다. 다음 그림과 같이 사용자가 3일 후에 응용 프로그램 사용을 중지하면 평판 손실이 발생합니다. (빨간색 줄은 평판이 누적되는 동안 평판을 획득함).



평판은 초반에는 서서히 떨어지고 시간이 지남에 따라 특정 기초 수치로 빠르게 떨어집니다. 다음 번에 이 사용자가 동일한 앱을 활성화하면 더 이상 0에서 시작되지 않습니다.

Comprehensiveness

DREP 평판 프로토콜은 B측뿐만 아니라 C 최종 사용자에게도 중요합니다. 상응하는 우대 조치와

교환하여 평판 수집을 통해 생태 폐 루프를 형성하여 사용과 소비를 더욱 촉진합니다.

3.3.3 평판 시스템은 ID를 보완하고 향상시킵니다.

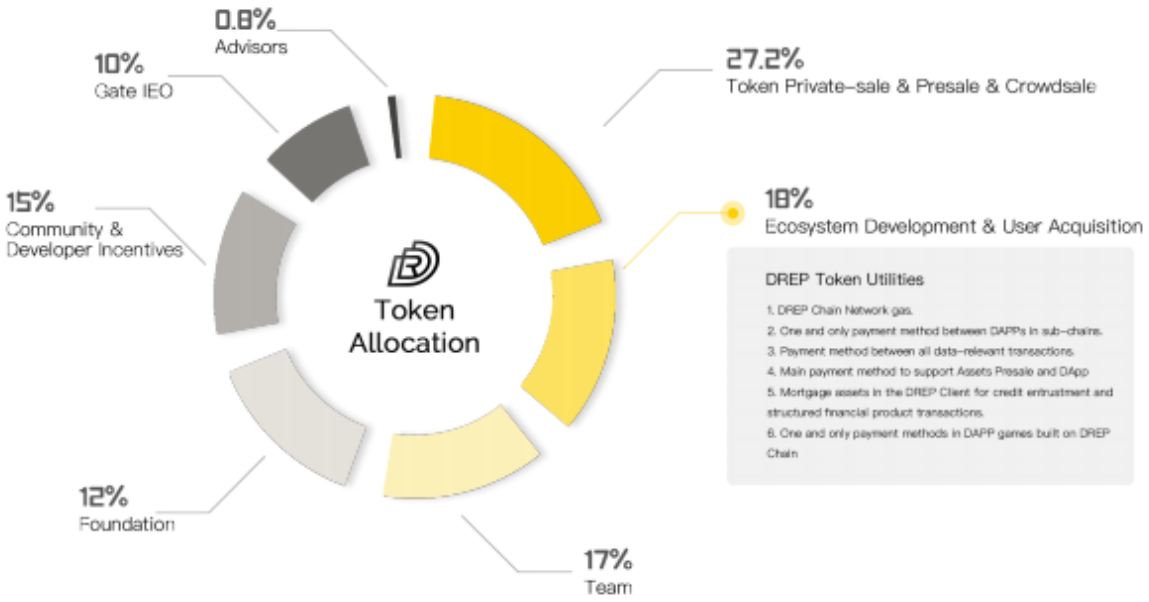
DREP의 평판 프로토콜은 포인트 시스템을 보완, 확장 또는 교체할 뿐만 아니라 다양한 응용 프로그램에서 생성 된 생태계가 최종 사용자의 평판 이미지로 통합됩니다.

정확한 타겟 추천 및 마케팅 측면에서 응용 프로그램에서 사용자의 활성 정보를 얻는 것만으로는사용자의 완벽한 이미지와 관심을 묘사하기에 충분하지 않습니다. 그러나 평판 이미지를 요약하면 큰 데이터 및 기타 방법을 통해 사용자의 관심 분야 또는 사용자의 습관에 적합한 사용자 유형을 파악한 다음 사용자의 개인 정보 침해 주장을 피하면서 사용자의 요구 사항을 충족시킬 수 있습니다.

DREP Tokenomics

DREP은 총 100억의 토큰을 발행했습니다. 토큰의 분포 계획은 다음과 같습니다.

- Ecosystem development and utility scenarios: 18%
- Community and developer incentives: 15%
- Token private sale / pre-sale / public offering: 27.2%
- IEO: 10.1%
- Team: 17%
- Foundation: 12%
- Advisors: 0.8%



DREP 토큰의 사용 시나리오는 다음과 같습니다.

- 네트워크 수수료
- 서브 체인 간에 크로스 체인 트랜잭션의 유일한 지불 수단
- 네트워크의 모든 데이터 관련 트랜잭션에 대한 지불 수단
- DREP SDK 의 자산 사전 판매 및 응용 프로그램 Gametopia 적용에 사용되는 주요화폐
- 신용 거래 및 구조화된 금융상품 거래를 위한 DREP 클라이언트의 담보 자산
- 향후 DREP 게임 내 결제 방법 및 자산 거래
- DREP SDK 와 통합된 일부 DApp 또는 플랫폼에서 DREP 토큰을 직접적으로 사용 후 제품 논리를 검증