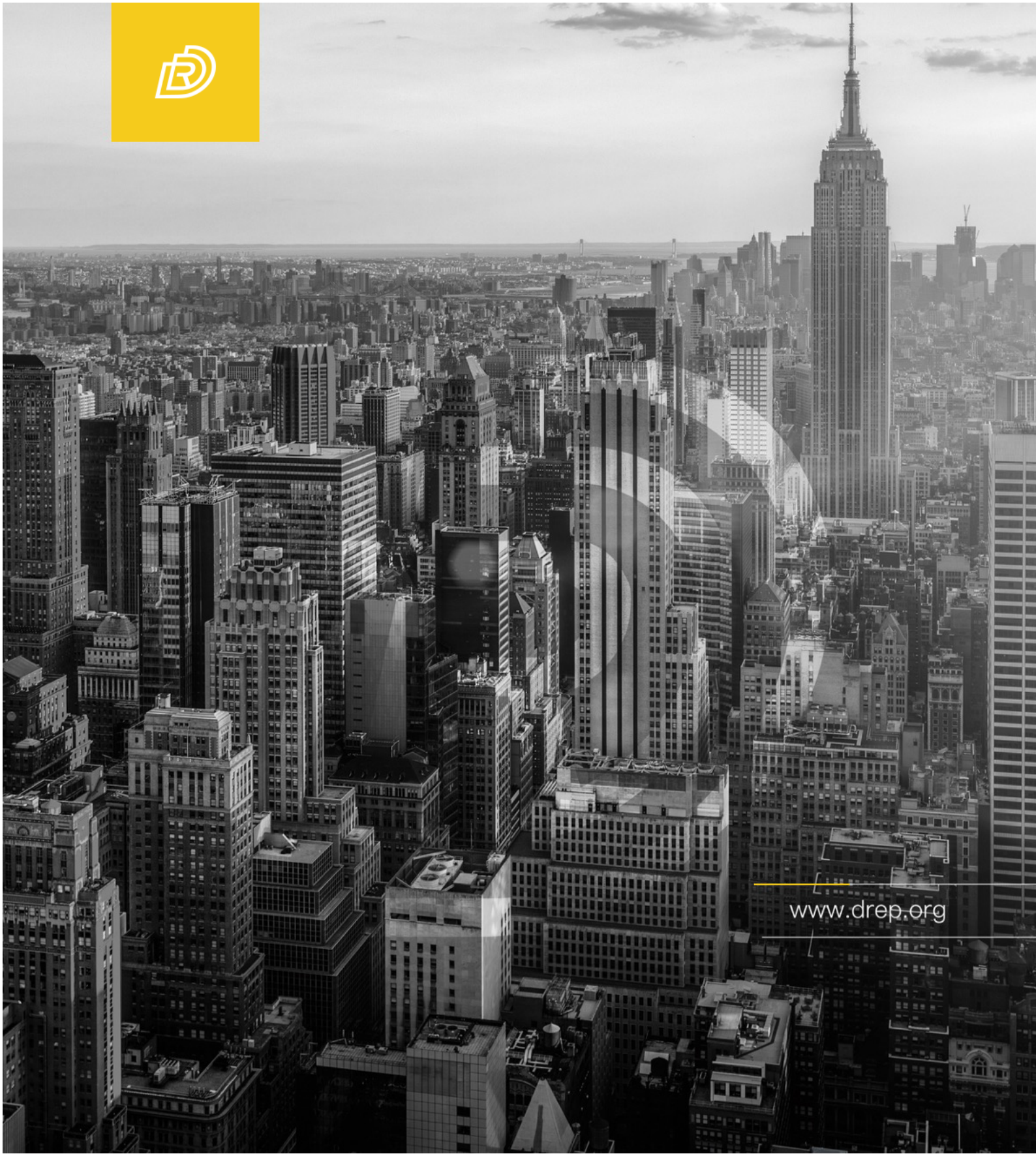



# WHITEPAPER

链上数据生态系统

# 重要声明

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.

# 摘要

如果说，互联网实现商业化的原因是连接了信息；那么区块链可以跨越互联网、物联网的原因是，可以打破数据孤岛，连接一切。

目前的区块链商业环境仍处于数据割据状态。一方面，基础公链和行业公链为了追求竞争优势最大化而建立闭环生态；另一方面，DApp（去中心化应用）为了触及更多用户，则需要针对不同公链开发独立的版本，用户及数据体系被割裂。基于此，DREP 的首要目标是通过 DREP 去中心化 ID、跨链设施及 DREP SDK 形成“连接器”，支持 DApp 一键发布多链版本，跨平台账户数据一体化，并在数据共享过程中通过同态加密进行隐私保护。

在区块链技术从研究走向应用，从应用走向易用的进程中，企业侧对技术的认知和需求往往滞后，需要被发掘和引导。这一阶段，无论是区块链基础设施，还是工具化应用，能够快速切入市场的只有高度产品化的解决方案，能够解决细分领域的痛点问题，具备较高的技术投入产出比，同时能最大程度不损害用户体验。DREP 的市场化路径是打造灵活易用的 “工具箱”，采用可定制化的双层公链架构，将较成熟的解决方案开发为接口式 API 和插件，并通过 DREP SDK 打包垂直领域的产品化组件。

**DREP 的发展愿景是：**

- 高并发，而不止高并发，我们的目标是让并发性高低不再成为限制商用的瓶颈。
- 人性化，而不止开发灵活性与隐私保护，我们的目标是让 B 端和 C 端用户无感使用区块链服务。
- 商业化，而不止 DApp 与企业级服务，我们的目标不是复制互联网，而是连接一切数据孤岛。

# 什么是 DREP

**DREP 致力于打造基于区块链技术的“连接器”和“工具箱”，提供兼具灵活性、易用性和用户无感化的解决方案。**基于 DREP 底层公链、DREP 去中心化 ID 系统、DREP 声誉协议层及 DREP SDK，可以构建开放式链上数据生态，打破公链生态割据的现状。

区块链技术发展至今，一方面层出不穷的区块链项目在可拓展性、安全性、隐私性等方面不断迭代解决方案，却仍旧只能扶植规模有限、类型匮乏的应用基于区块链底层做开发；另一方面，具备一定经营规模的企业，很少将区块链技术真正应用到大型商业场景中，也很难为区块链领域带来真实的用户增量。

**因此，DREP 主要解决三类问题：**

- 公链性能不足，开发者体验差。
- 公链生态割据，区块链用户基数小。
- 区块链技术与实体企业需求脱钩，落地难度大。

**DREP 主要提供的技术解决方案如下：**

- DREP 公链是由 DREP 开发团队完全自研的一条高性能公有链，兼容 EVM 和 WASM 格式的智能合约，具有双层架构：稳定的根链及可定制的子链系统。
- DREP 提出的智能管道技术（Smart Pipeline）可以在区块链虚拟机和外部应用之间传输数据，提升批量数据处理能力，高效率、强拓展、零 Gas，解决智能合约（Smart Contract）无法解决的现实需求。
- 为提升网络效率，减少传输开销，DREP 使用了基于 Secp256k1 椭圆曲线的 Schnorr 多重签名算法。
- 为实现数据串联和隐私保护，DREP 设计了基于 HMAC 算法的去中心化 ID 系统，形成一个主 ID 加多个子 ID 的分层体系。允许用户通过 DREP 客户端，对中心化及去中心化平台上的数据和资产，进行一站式管理。
- 为强化数据隐私保护，DREP 采用同态加密的方式，对用户认定为隐私的信息进行数据处理。
- 为提供 DREP DID 的长期持有价值，DREP 推出了声誉系统，包括通用声誉协议、声誉管道接口、声誉数据上链与算法库、声誉激励机制、声誉账户管理与虚假检测等。
- 为降低技术使用门槛和教育成本，DREP 研发了 API、Plug-in（插件）及针对垂直行业的 SDK，可支持 DApp 团队一键发布多公链资产支持版本，内置钱包及资产交易平台，基于共享 DREP ID 获取多公链用户，无感转化各类数字资产持有者成为其平台用户。
- DREP 代码风格是向面向 Service 的编程，类似于 Java 的 Spring 容器开发。大部分区块链项目的代码中，各个模块之间耦合比较严重，DREP 这种做法让各个模块充分解耦，代码可以轻松重构，逻辑清晰。

在 DREP 主网正式发布前，DREP 测试网络将经历 4 次版本迭代，分别代表开发团队 4 个重要的工作节点，也代表 DREP 产品、市场及商务团队在与合作企业的沟通过程中，不断挖掘核心痛点、升级技术方案、优化产品体验，推进提升 DREP 技术产品体系的市场化和竞争力。DREP 的 4 版测试网络将分别以 Darwin（达尔文）、Riemann（黎曼）、Euler（欧拉）和 Planck

（普朗克）命名，以致敬四位科学家在人类发展进程中的伟大贡献，同时象征 DREP 团队在技术研发和商业应用道路上迎难攻坚、不断求索：

进化之源，Darwin；

破局之点，Riemann；

无穷之道，Euler；

常量之变，Planck。

# DREP 如何解决问题

## 2.1 公链性能差，开发者体验差

TPS（Transaction Per Second，每秒处理交易数量）是制约公链商业化路径的一大发展桎梏。第三方支付 Paypal 的 TPS 目前在 100 数量级，而 Visa 信用卡可达 2000 左右[1]。然而 Bitcoin 和 Ethereum 的 TPS 仅可达 10 左右[2]。这不仅制约了区块链支付方面的发展，同时也增加了 DApp 开发者开发的难度。

随着 DApp 的不断发展，链上应用数据量迅猛增加，EOS 的 RAM 已使用 62%[3]，并随着时间不断增加使用比例与资源价格。这对公链平台而言可谓雪上加霜。基于并发性的问题，已不可能仅仅依靠协议层的智能合约来记录 DApp 数据[4]。

因为区块链存在不可能三角[5]：去中心化、可拓展性、安全性这三者无法兼容，所以公链无法在不牺牲去中心化和安全性的前提下，提升链上的 TPS。因此 DREP 创新提出了类 Layer2 拓展优化方式——智能管道（Smart Pipeline），以提升数据批量处理能力，并为开发者提供相应开发工具以突破现有公链的开发制约性。

### 2.1.1 DREP 智能管道提升数据批量处理效率

智能管道（Smart Pipeline）是 DREP 团队提出的一种崭新的区块链应用模式，在不影响安全性的基础上，具有高效、零 Gas 消耗、拓展性强的诸多优势，解决智能合约无法解决的现实需求。

智能合约（Smart Contract）在 Ethereum 等平台得到广泛应用的同时，其数据容量、Gas 消耗、缺乏主动调用功能等诸多问题为开发者所诟病，限制了大型 DApp 的开发。

DREP 智能管道是数据传输的“管道”，在区块链虚拟机和外部应用之间传输数据：区块链客户端将实时数据通过智能管道传输给外部应用，外部应用执行后将结果通过智能管道实时返回给区块链客户端。

这些智能管道能够被插入于区块链执行区块的各过程中，并且可以根据需要选择插入的位置执行相应代码，提升执行效率。

**智能管道的优势：**

---

[1] Kiayias, Aggelos, and Giorgos Panagiotakos. "Speed-Security Tradeoffs in Blockchain Protocols." *IACR Cryptology ePrint Archive* 2015 (2015): 1019.

[2] Kogias, Eleftherios Kokoris, Philipp Jovanovic, Nicolas Gailly, Ismail Khoffi, Linus Gasser, and Bryan Ford. "Enhancing bitcoin security and performance with strong consistency via collective signing." In *25th {USENIX} Security Symposium ({USENIX} Security 16)*, pp. 279-296. 2016.

[3] *https://coinatory.com/2018/09/07/why-dapp-on-eos-is-not-profitable-for-developers-part-1/*

[4] Olga Kharif,https://www.bloomberg.com/news/articles/2017-12-04/cryptokitties-quickly-becomes-most-widely-used-ethereum-app

[5] Wang, Wenshi. "A Vision for Trust, Security and Privacy of Blockchain." In *International Conference on Smart Blockchain*, pp. 93-98. Springer, Cham, 2018.

- **更“智能”**：智能管道部署上链后，可以根据条件自动触发执行，相比智能合约条件范围更加广泛，执行更难受到干扰，非常利于复杂事务的执行。
- **零 Gas 消耗** :智能管道的应用在执行时，相比智能合约的一大优势是无需消耗 Gas。零 gas 消耗并非零责任，所有智能管道运行代码需要开源接受监督。同时智能管道消耗计算资源主体并不在相应子链上，而是由智能管道代码提交方提供计算资源，即便出现漏洞，也不会影响相应子链的性能。
- **编程语言无局限性**：智能管道采用 WASM 虚拟机进行交易的执行，用户可以使用多种编程语言进行代码编写，之后转成 WASM 指令。随着 WASM 的不断改进，其支持的语言种类将逐步增加，代码效率也会得到相应提升，不会影响区块链的执行。
- **满足复杂应用的需求**：智能管道的应用没有受到 Gas 等限制，可以支持区块链实现更复杂的逻辑。在精心设计后，带有智能管道的区块链可以和其他应用或者服务进行交互，满足大型复杂应用的需求，制作已有区块链无法支持的应用。

### 2.1.2 DREP 双层架构及可定制化子链

DREP 链采用主链-子链的双层架构体系，在不影响去中心化程度和安全性的同时，提升了可拓展性，强化了区块链底层的效率。在 DREP 已开源的测试网络中，经 2019 年 1 月 8 日公开网络测试，**DREP 链 TPS 峰值超过 12000**，本次测试环境如下：

- 出块时间：10 秒-15 秒

  各区块大小：没有限制

  结构：1 个主链，10 个子链。

  每个链的结构：7 个挖矿节点，10 个普通节点。

  测试网地址：drep.me

**DREP 主链与子链可以分别独立处理不同场景下的不同交易、允许多种共识机制与数据存储的差异化共存，提高了并发性的同时为不同场景的接入提供了兼容性支持。**因此无论是区块链应用，还是传统企业或平台接入，都可进行进行相应子链定制，最大程度降低接入门槛。

### 2.1.3 DREP 改进共识机制

PBFT 是一种安全高效的共识机制，在 hyperledger 等联盟链中已得到应用[6]，但已有的 PBFT 共识机制在共识效率等方面不足以满足公链需求。DREP 通过 Schnorr 多签名[7]算法强化 PBFT，整合大量签名为一个签名，在存储和网络传输等方面提升 DREP 链效率，减少网络传输开销。由此，PBFT 可以应用于 DREP 公链系统中。

---

[6] https://www.hyperledger.org/wp-content/uploads/2017/08/Hyperledger_Arch_WG_Paper_1_Consensus.pdf

[7] Schnorr, Claus-Peter. "Efficient identification and signatures for smart cards." In *Conference on the Theory and Application of Cryptology*, pp. 239-252. Springer, New York, NY, 1989.

### 2.1.4 DREP 开发者工具

DREP 将提供 DApp 开发与子链定制化开发的一系列开发资源，包括 Docker、IDE 等上层工具以及控制台和其他底层服务，同时拥有浏览器、水龙头、测试网络等测试工具，方便开发者基于 DREP 进行开发。

DREP Docker 具有适于快速入门，易于安装部署等优势，便于接入；而 DREP 控制台具有可编程可交互的特性，支持脚本操作，有利于开发者应用；另有 RPC 接口与 JS 库可用于多种场合的节点访问等诸多功能。

## 2.2 公链生态割据，区块链用户基数小

区块链领域最激烈的竞争在于“主链”[8]，每条主链都在竭尽全力成为区块链底层的龙头，进而成为领域内的苹果与微软。在这种氛围中，各条公链之间从底层架构到上层 DApp 之间壁垒森严，将原有不多的区块链用户进一步分割为 ETH 用户、EOS 用户等等。这将必然带来公链发展的“囚徒困境”。

DREP 希望透过 DREP ID，将原有分散在各条公链的用户账户进行整合，并将范围进一步向传统平台推广，让更多用户无感进入区块链，解决用户基数的问题。这样，开发者也能够突破公链间的壁垒与区块链圈的限制，获得更多的用户。

### 2.2.1 DREP ID 打通数字资产

DREP ID 可通过 DREP 客户端将各类加密数字货币予以整合，允许用户通过 DREP 客户端进行一站式管理。将不同平台的地址绑定在 DREP ID 上，即可通过跨链互操作等设计进行不同平台账户转账等管理。

这一功能不止局限于区块链应用内，通过 DREP ID 还可以与 DREP 合作的传统（中心化）平台等进行跨平台管理，在不改变原平台的数值系统、积分系统、经济系统等基础上进行资产与数据整合、信息加密保护等，形成完整的去中心化闭环生态。

基于此方案，DREP ID 可真正支持跨链超级 DApp，允许 DApp 开发者与用户不受底层链平台的局限，进行各类主流币的互相转账，也可以选择去中心化交易所进行 Token 兑换。这会提升用户在 DApp 中的使用体验，同时为 DApp 开发者拓展用户范围，减少重复开发等提供重要的帮助。

### 2.2.2 DREP ID 串联用户信息

区块链难以学习和使用的一大特征为毫无理解性的 20 位以上公钥地址，目前仅有 EOS 等极少数公链认识到这一点，但 EOS 每个地址的注册均需要花费，当地址较多时记忆仍然不便，同时花费不菲。

DREP 提出使用 Alias（别名）产生用户可以理解的账户名称，降低使用区块链的门槛，以一

[8] Lianos, I. "Blockchain Competition–Gaining Competitive Advantage in the Digital Economy: Competition Law Implications." Oxford University Press, 2019.

个名字管理大量地址，减少消耗。DREP 使用的 Alias 并不需要记住 20 位以上的公钥地址，而是用户可自行申请的昵称，存储于区块链上。

对于已有的账户，将其地址链接到 DREP ID 上后，将无需再记忆相关复杂信息。而通过 DREP ID 产生新的子账户，则不需要记忆地址信息，方便用户使用。

Alias 不仅是用户 DREP ID 的记号，在不同子账户中的行为，均可通过 DREP 的 Reputation Protocol 与之链接，形成用户的可信度标记，让用户重视自身的“第二身份”——DREP ID。

### 2.2.3 DREP ID 保护用户隐私

一些中心化平台为了获取用户数据，往往是未经用户同意进行分析和转卖，甚至通过对用户诱导付费购买相关信息。在 DREP ID 生态中，用户可以自行决定不同数据是否公开。对于涉及隐私的用户信息，可以通过有偿授权的方式为第三方使用，用户可以从中获得 DREP 通证作为补偿，第三方机构可以通过用户的声誉评价等因素提升数据获取质量，同时降低数据获取成本。

在中心化平台进行登录时，服务器将获取用户登录信息、登录账号甚至更多的信息。当使用关联账户这种更加方便形式时，甚至可以在未经用户同意下刻画出用户形象。DREP ID 将结合第三方登录的便利性，同时避免中心化平台单方面获取用户隐私的弊病。用户可以选择平台获取哪些登录信息，以何种身份登录，不需要记录大量不同账户信息的同时保护自身隐私不受侵犯。

## 2.3 区块链技术与实体企业需求脱钩，落地难度大

区块链被寄予了改变生产关系的厚望，但由于其技术合集面向的问题种类有限，自身效率也无法与中心化服务器比拟，同时缺乏联通区块链技术侧与实体产业需求侧的人才，区块链技术企业在探索实体产业应用落地的道路上困难重重。

针对与实体产业需求对接的问题，DREP 认为不应当做“闭门造车”的区块链技术团队，而是在这个仍需要进行市场/客户/用户教育的阶段，进行垂直领域的高可用性工具组件研发，了解真实的开发痛点和难点，而不是臆测或预测需求。

DREP 主要的解决方案分为两大类，第一类是把 DREP 较成熟的技术解决方案开发为可直接调用的 API（应用程序编程接口）和 Plug-in（插件），因此大大降低应用端/企业端的对区块链的认知成本、开发难度和使用门槛；第二类是针对垂直领域进行 SDK（软件开发工具包）定制化开发，解决开发过程中的特定问题，形成完整的垂直领域技术解决方案。

### 2.3.1 DREP API 及 Plug-in 降低使用门槛

DREP 提供相应的 API，不需要传统平台进行大改去中心化，只需调用 API 即可适应不同语言的区块链化开发。
针对更加精确而复杂的平台区块链化需求，DREP 亦可提供相应 Plug-in 帮助垂直领域开发。
DREP API 和 Plug-in 的优势在于：

1. 无需理解整个区块链即可进行针对性开发，便于功能的扩充。
2. 支持并行开发，调试修改等开发过程非常方便。

3. 将实际问题以最直接的方式转换到区块链进行解决，将使用门槛降到最低。

### 2.3.2 针对垂直行业打造的 DREP SDK

DREP SDK 是由 DREP 团队研发，支持各类 DApp 上链的开发者工具组件。DApp 研发团队将可以一键发布多公链资产支持版本，内置应用钱包及资产交易平台，基于共享 DREP ID 获取多公链应用用户，无感转化各类数字资产持有者成为应用受众，打造超级 DApp。

超级 DApp 指：DApp 发布不再受限于某一个公链生态，不再需要针对 ETH、EOS、TRON 等进行多个版本的研发，而是通过 DREP SDK 打通所有数字资产，使区块链全行业用户可以无门槛的进行支付、交易、抵押等行为。同时传统 App 用户可以无感化迁移至区块链 DApp 版本，用户教育成本大幅降低。

以游戏行业为例，DREP 区块链游戏 SDK 包括以下内容，并随着未来发展不断增加：

1.游戏账户模块，核心优势是基于跨链的 DREP ID，打破公链用户生态割据现状；

2.支付交易模块，核心优势是通过内置支付、交易引擎，进一步优化数字资产交易体验；

3.数值运营模块，游戏运营数据以及游戏内部经济系统都可实现数据可视化、透明及可配置。

# DREP 技术架构

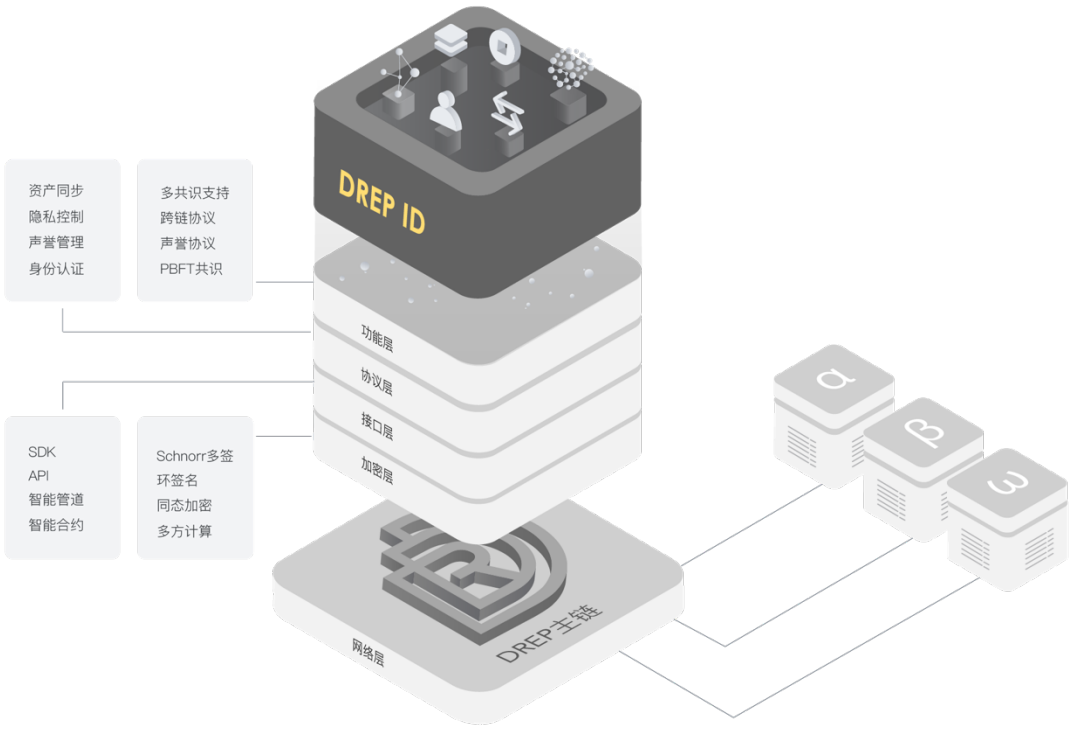
## 3.1 DREP 公链

DREP Chain 是由 DREP 开发团队完全自研的一条高性能公有链，兼容 EVM 和 WASM 格式的智能合约，使用双层架构，由根链和子链组成，根链主要负责子链数据同步和 DREP 代币的交易等，子链便于 DApp 或企业基于 DREP 链开发自己的区块链系统，可以独立发行代币，使用智能管道、智能合约、资产跨链、声誉数据共享等功能。

DREP Chain 在共识选取方面，以效率优先，所以在第一版测试网络中 DREP 选择了改进的 PBFT 作为子链和根链的共识机制，在后期根链会逐步转化成为带声誉机制的 POS 机制。

DREP 改进传统的 PBFT 共识机制，引入了基于多重签名的 PBFT，提升 DREP 链真实效率。区块链的效率不仅仅体现在 TPS 上，更体现在存储和网络传输过程中。原 PBFT 协议中参与者需将信息的签名传给 Leader，Leader 整合签名进入区块头，存储多个签名将增加区块头的大小。DREP 使用了基于 Secp256k1 椭圆曲线的 Schnorr 多签名算法，最终只产生一个签名，大大减小了签名的长度，从而减小了区块头大小，减轻了存储开销和网络传输开销。

**DREP 技术架构如下：**



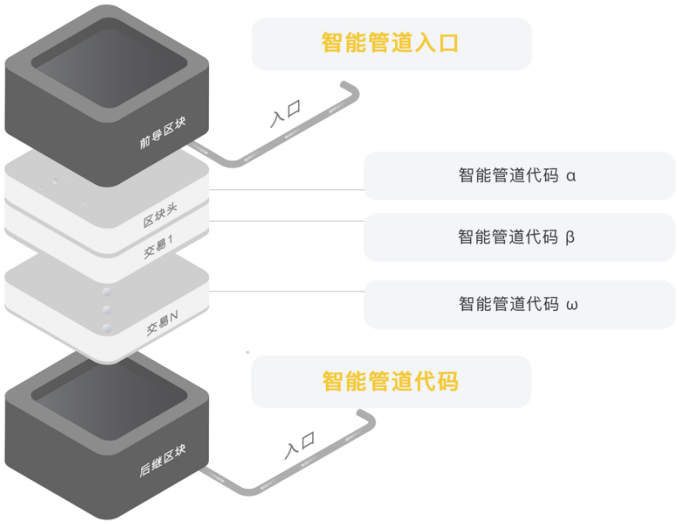

### 3.1.1 DREP 智能管道

为了提升数据处理能力，DREP 创新性提出智能管道概念，即：在区块链虚拟机和外部应用之间传输数据，以提升批量数据处理能力。相比在 Ethereum 等平台上广泛应用的智能合约（Smart Contract），智能管道的核心优势为高效率、强拓展性以及不产生 Gas 费用。

**智能合约的问题主要体现在：**

- 打包区块最大数据容量过小。根据 ETH 设计，当前单个区块最多的 Gas 使用量为 3,141,592 Gas，可以反推出其附带数据量不能达到 1M，[9]这就意味着 DApp 不能携带大量数据，否则会导致区块阻塞。
- 智能合约的读写与计算消耗 Gas 过高，开发者不敢使用在传统平台非常常用但在区块链上消耗巨大的算法，限制了 DApp 的设计。
- 没有主动调用功能。智能合约无法自主执行以定时任务为代表的复杂任务，需要外部脚本参与。

**智能管道的原理如下图所示：**




区块链执行区块时，会将区块中的事务，逐一放进虚拟机进行执行。而在每个事务的执行前后，均可插入智能管道。智能管道就像程序的断点一样，客户端根据配置激活一部分管道（断点）。当客户端执行到一个被激活的智能管道（断点）的时候，将自发启动一个 stop-the-world 的过程，将实时数据通过这个管道将实时数据传输到外部应用，由外部应用处理数据，外部应用处理数据后，将结果通过智能管道传给区块链客户端，客户端将这些数据存入数据库，完成数据上链。这个过程规避了大量数据在虚拟机中处理的弊端，同时由于智能管道经过 DREP 的深度优化，其传输过程不仅不影响运行效率，反而可以提升数据处理效率。

DREP 智能管道的应用由 WASM 指令集组成，通过区块链进行分发，可以在不同的子链上选择不同的应用执行，也可以自主编写应用经审核后执行。

### 3.1.2 DREP 跨链协议

DREP 的跨链协议突破了传统跨链只能进行资产转移的思维定式，将声誉（征信/忠诚度）等重要个人身份相关的行为数据也进行跨链同步与迁移，通过同态加密进行安全保护与使用。

[9] https://ethereum.stackexchange.com/questions/1106/is-there-a-limit-for-transaction-size/1110

根据不同需求，DREP 采用同构与异构两套跨链方案，以应对不同架构下性能和成本的平衡：

- **同构跨链**：DREP 主链与子链之间通过轻量化同构跨链协议相互连接，用户可以通过钱包即时看到不同跨链平台之间的状态变化。
- **异构跨链**：分布式私钥控制技术将 DREP 体系之外的链甚至传统平台跨链连接到 DREP 生态中，达成安全的异构跨链，将声誉协议的应用范围拓展到多种平台。

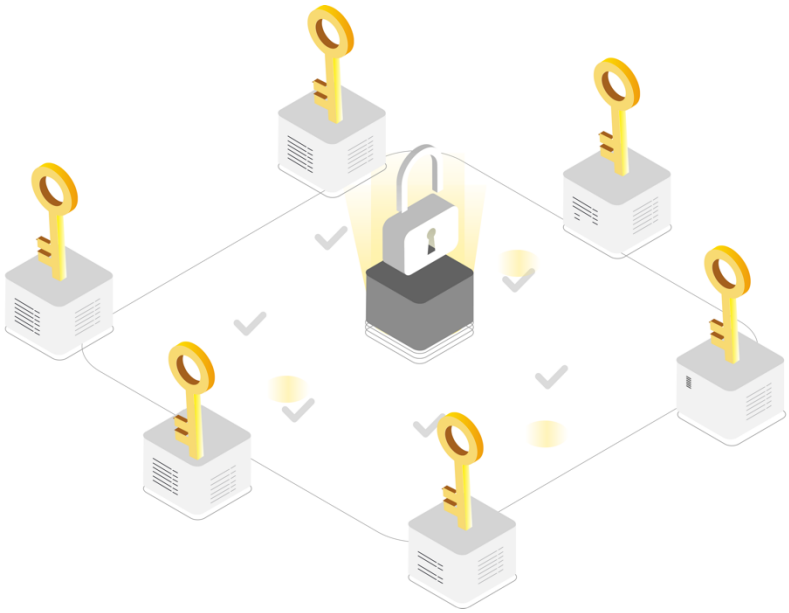
基于同构与异构两种跨链技术，将处于不同 DApp 的 Token 和声誉数据均通过跨链技术集成在主账户中，形成一个多层次、立体化的用户声誉情况列表。

除此之外，DREP 也在考虑将合作伙伴的用户行为也进行声誉化，在跨域要求的安全性控制条件下将声誉扩展到各个不同的系统，使声誉走出区块链的范围，形成广域声誉生态。

**分布式私钥控制**[10]

分布式私钥控制通过去中心化技术，将跨链资产用多个私钥加以控制，原持有者仍然拥有所有权，只是其单一私钥不能取出资产而已。想要回归资产，需要向对应链加以申请获得足够私钥。

举例，用户 Alice 希望能够将 1 个原链币转成另一链币。跨链的若干节点（分片/超级代表委员会都可以）在原链上维护一个多签账户，将私钥分割且分别控制，任何单一节点不能取得这 1 个原链币，只有获得足够的私钥才能获得 1 个原链币的控制权。



当 Alice 将 1 个原链币打到跨链掌控的多签账户时，在跨链相应的同步放出等同于 1 个原链币的跨链币，再和持有已将另一链币转化等价跨链币的节点进行交易。当 Alice 需要将跨链币要重新回到原链时，需要先将跨链上的资产锁定，然后在原链中将同等数量的原链币释放。

分布式私钥控制过程安全性较好，同时因为在跨链上放出代币，所以支持智能合约特别是多

[10] Kate, Aniket, and Ian Goldberg. "Distributed private-key generators for identity-based cryptography." In *International Conference on Security and Cryptography for Networks*, pp. 436-453. Springer, Berlin, Heidelberg, 2010.

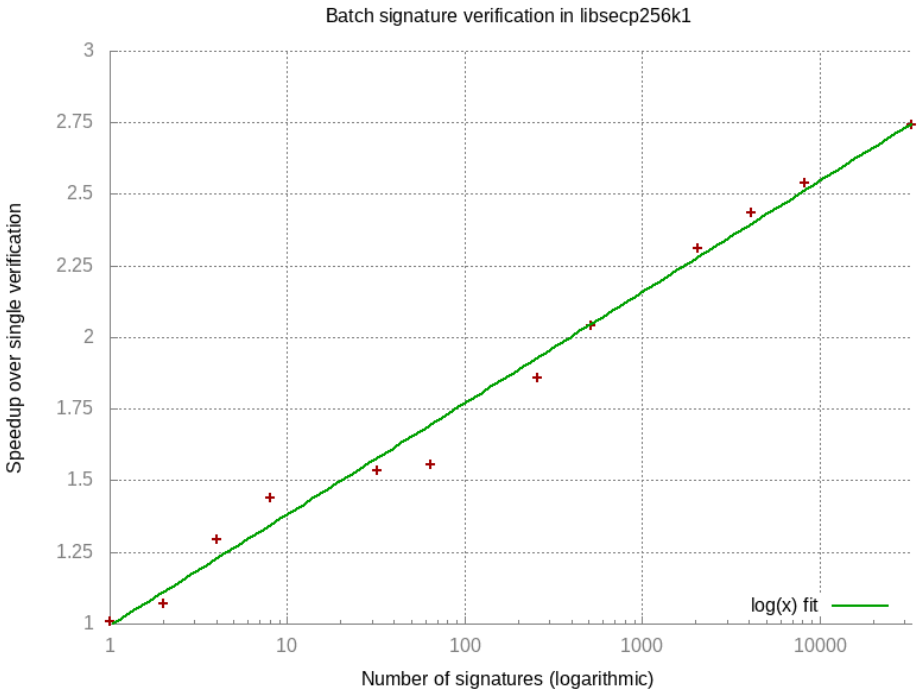
币种复杂合约，不受原链本身是否能进行智能合约影响。

### 3.1.3 DREP 隐私保护设计

#### Schnorr 多重签名

DREP 引入了基于多重签名的 PBFT 机制。传统 PBFT 协议需要参与者将信息的签名传给 Leader，然后 Leader 将这些签名放进区块头。但存储多个签名将增加区块头的大小，影响网络传输效率。DREP 使用了基于 Secp256k1 椭圆曲线的 Schnorr 多签名算法，明显提升了区块链效率。

**BIP-Schnorr 签名中对 Schnorr 签名性能的测试结果如下：**[11]




不同于其他签名形式，Schnorr 多重签名最终只产生一个签名，大大减小了签名的长度，从而减小了区块头大小，减轻了存储开销和网络传输开销。

另外，当未来需要增强隐私性交易需求时，除了环签名之外，Schnorr 签名亦可提高隐私性。

#### 同态加密与隐私保护

DREP 链的运行过程中，必然会遇到将信息传递给第三方的情况——如内部的智能管道和外部的数据共享。在这些过程中，有可能会出现用户隐私在环节内被泄露等情况，不利于用户的 ID 安全。为此，DREP 采用同态加密的方式，在用户认定为隐私的信息进行数据处理中，保护数据本身的隐私安全。

[11] https://github.com/sipa/bips/blob/bip-schnorr/bip-schnorr.mediawiki

同态加密使用的 Paillier 算法[12]，即基于二次整数群的 n 次剩余类方法进行加密。

对于原始信息 m∈(0,n),选择随机数 r∈(0,n),根据生成的密钥对：公钥(n,g)私钥(λ,u),进行加密，$C=g^m r^n \ mod n^2$ 得到密文 C。

密文 C 满足加密同态和混合乘法同态性，即：

- **加法同态性**

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

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

- **混合乘法同态性**

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

从而在加密后可以进行多种数据处理，将处理结果返回给用户，用户用私钥解密就能得到与明文数据处理相同的结果，而不存在数据泄露的可能。

在此之上，还可以进行同态加密签名，在内容中加入同态签名，在数据处理过程中得到是否发生误处理及欺骗等行为，确保自身数据得到正确的处理。

**安全多方计算[13]**

在分布式私钥控制与环签名等涉及多人共同分享秘密的过程中，需要遵循尽可能不出现完整秘密的原则，故 DREP 选择安全多方计算以保护数据安全，仅当用到时出现完整信息。

安全多方计算解决的是以下问题：n 个人分别持有隐私 x1，x2……xn，共同计算特定函数 y=f(x1,x2,……xn)，同时 n 个人无法得知其他人的隐私。考虑到现实中存在恶意节点会竭尽所能获取其他参与方的隐私信息。安全多方计算协议要求不论参与者是否有恶意，所有参与方都无法获得输出结果以外任何的附加信息。

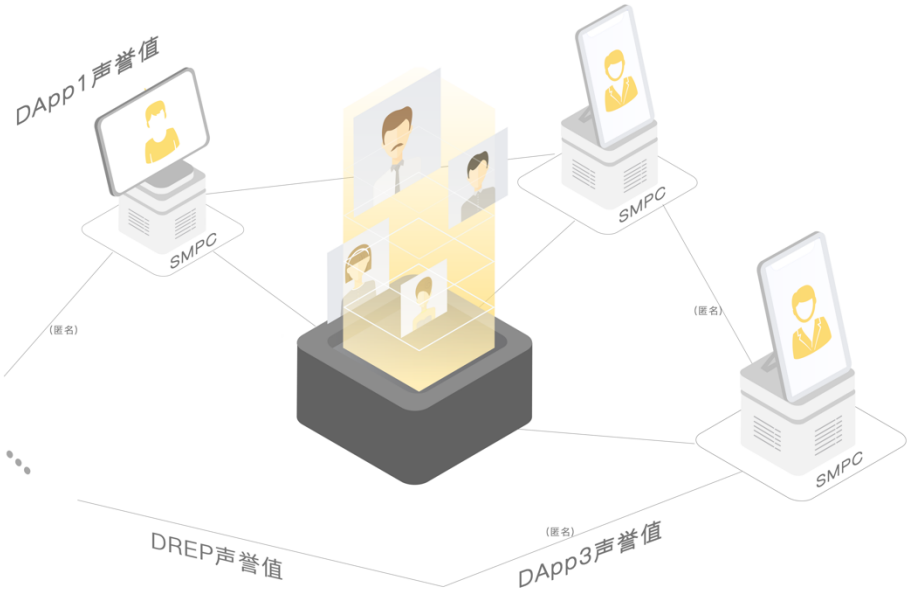
DREP 考虑通过同态加密、bulletproof[14]等措施进行安全多方计算，以声誉计算为例。

---

[12] Paillier, Pascal, and David Pointcheval. "Efficient public-key cryptosystems provably secure against active adversaries." In *International Conference on the Theory and Application of Cryptology and Information Security*, pp. 165-179. Springer, Berlin, Heidelberg, 1999.

[13] Yao, Andrew Chi-Chih. "Protocols for secure computations." In *FOCS*, vol. 82, pp. 160-164. 1982.

[14] Bünz, Benedikt, Jonathan Bootle, Dan Boneh, Andrew Poelstra, Pieter Wuille, and Greg Maxwell. "Bulletproofs: Short proofs for confidential transactions and more." In *2018 IEEE Symposium on Security and Privacy (SP)*, pp. 315-334. IEEE, 2018.




DREP 使用安全多方计算对各个 DApp 及 DREP 平台中的重要数据进行加密，即使传输中的数据被泄露，用户的原始数据也是安全的。安全多方计算也保证了传输数据的双方能安全的加密和解密数据。同时在 DREP 平台上，用户在每个 DApp 上的公钥，地址及数据都是相互独立且不可见的。

### 3.1.4 改进与优化

自主开发 DREP 链的重要原因，正是在于现有区块链主链的耦合性太强，不适于与企业已有系统无缝结合。同时很多高 TPS 的主链实际上如果出现高并发请求，配套性能无法满足现有需求。

**结构优化方面：**

DREP 将数据库、网络、共识等各个部分进行模块化开发，并装入各个容器，通过中间件进行模块化调用，实现各模块解隅。底层通过中间件可以自动实现容器的注册、启动、升级等一系列操作。对于子链开发者，DREP 链的底层代码逻辑清晰，可以轻松重构。除此之外 DREP 独创了路由和消息机制，将网络层和共识层完全解耦，使适用共识范围从 PBFT 拓展到 PBFT 以外的各种共识，方便子链自主开发共识。

**虚拟机优化方面：**

DREP 对已有 EVM 同样进行了改进，使之符合 DREP 链上业务的需求:

- 可以实现不同链上智能合约的执行
- 针对 DREP 的业务需求增加声誉相关指令
- 对 gas 定价进行了升级，使各子链能够根据配置与需求自动调整
- 基于业务需求，对底层数据库进行重新定制

**子链功能改进**

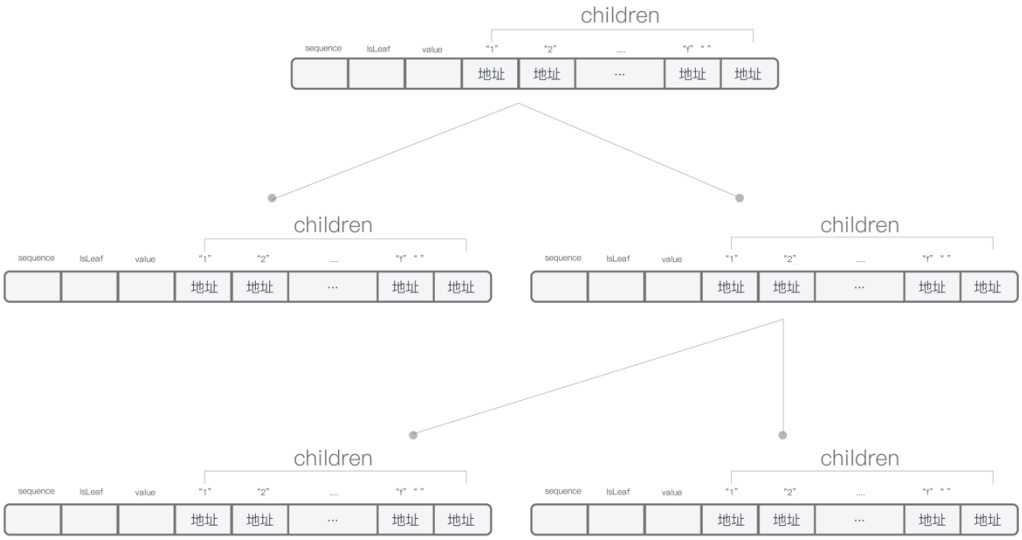
DREP 在子链数据同步到主链的过程中，如果出现子链数据错误，需要回滚，原 levelDB 不支持该操作，而自主开发的子链嵌套与回滚可以解决上述问题。

**数据库优化**

高并发请求时，对缓存等机制都会产生很大的压力，所以 TPS 很高和接受大量交易时保障性能并不等同。DREP 对缓存、数据库等进行优化和改进，并在 IRU cache 内部使用细粒度锁，使得在 TPS 达到 5000 时同样能够保证高性能。

DREP 链上的 LevelDB 数据库利用 Hash Patricia Trie[15]（哈希前缀树，以下简称 HPT）技术来保存用户账户状态和状态的变更。

HPT 是一种多叉树型数据结构，树上的每个节点由 Sequence, Value, Children, IsLeaf4 个属性组成。其中 HPT 的根节点 Value 属性保存了当前数据库状态的状态哈希值，用于区块校验。Sequence 属性则是得到特定的完整 Key 的必经之路。




当用户账户信息发生更改时，数据库会对 HPT 做出相应的修改以反映当前数据库状态的变化。根据用户账户的十六进制字符串 Key，数据库会从根节点开始进行深度搜索，直到找到某个叶子节点后，该搜索路径上的所有节点 Sequence 属性依次拼接后能够得到完整的 Key。

**HPT 的优点主要有两点:**

- 一是利用树状结构和哈希算法的不可逆性与极低冲突性，提高了数据库状态描述的便利性和可靠性。
- 二是利用数据库的键值设计和前缀树的数据压缩特性，极大提高了查询和修改状态的效率并减少了计算开销。每一条账户信息的修改后，只需要操作等于 HPT 深度的数目的树节点，即可完成对数据库状态的更新；一次事务中需要修改多条账户信息

[15] Kniesburges, Sebastian, and Christian Scheideler. "Hashed Patricia Trie: Efficient longest prefix matching in peer-to-peer systems." In *International Workshop on Algorithms and Computation*, pp. 170-181. Springer, Berlin, Heidelberg, 2011.

时，修改 MPT 所需要消耗的计算增长远远低于账户信息数量的增长，账户信息数量越多，能够节省的 MPT 计算量越为可观。

相比于以太坊项目中用于保存账户信息状态的普通前缀树结构，DREP 的 HPT 统一和优化了树节点的设计，抛弃了以太坊将树节点分为空节点、叶子节点、扩展节点和分支节点四类的做法，降低了前缀树的高度以及深度搜索时间，提高了 HPT 的查询和修改性能。

## 3.2 DREP ID

DREP ID 是用户数字资产管理的入口，同时也是 DREP 及合作应用平台上使用的数字化身份，也是用户在相应平台上产生数字形象的总和。

对于 B 端，DREP ID 是获得用户流量与高质量数据的入口，也是跨链资产交互的捷径，可接受多种不同货币/加密货币的支付。

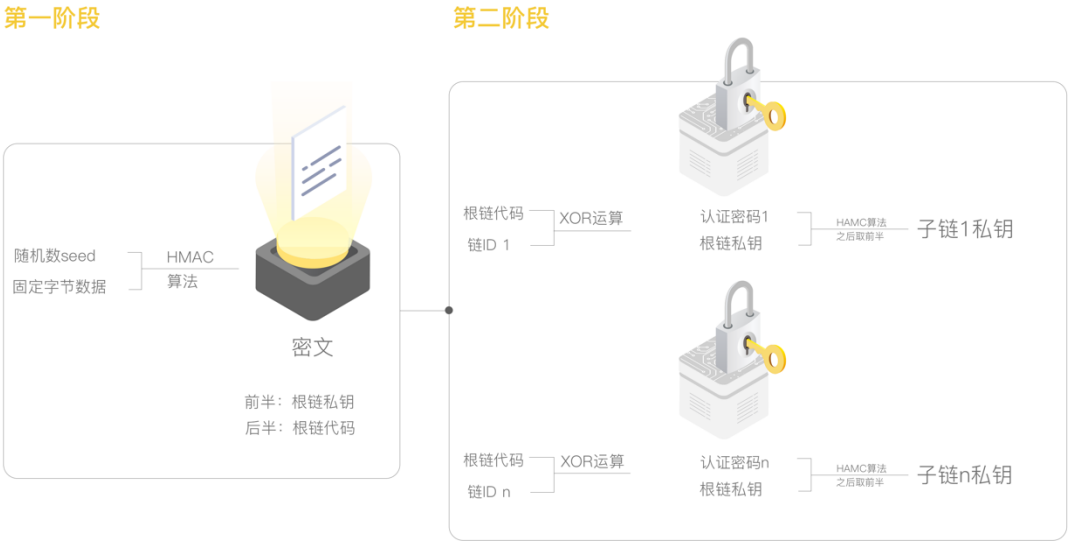
### 3.2.1 安全性

在 DREP 生态系统中每个用户拥有一个主账户和若干个子账户，通过 DREP ID 作为纽带，将不同应用上的声誉数据和资产串联，构建起一个用户完整的声誉画像。

在利用主账户生成子账户的过程中，DREP 通过 HMAC[16]（散列消息身份验证码）算法实现。

HMAC 的形式如下：

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




其中 K 是主账户密钥，m 是子链 ID，opad 与 ipad 为特定常量。通过主账户的私钥和相应

[16] rfc2104, https://tools.ietf.org/html/rfc2104

子链 ID 产生各子账户的私钥，进而通过主账户得以控制各应用子账户。其安全性在于：

- **主钥控制**：用户生成和获得子链账户的私钥需要同时利用对应主账户的私钥，身份验证码和子链 ID，因而极大保证了子链账户私钥的安全性。
- **不可链接性**：在不对称加密保护下，不论主链子链，各个链上的账户之间无法逆向关联，彻底保证了用户链上信息的匿名性。

**相比于 BTC 的 HD wallet，DREP 的 HMAC 具有以下优势：**

- **地址长度可变，安全性更高**

  DREP 采用了 SHA3 里的 SHAKE256（SHAKE=SHA+keccak）算法[17]，对公钥进行 Hash，可设定任意的输出地址长度，取得性能与安全更优点。

- **更少的计算开销**

  HD wallet 中需要生成大量的子私钥，用来定位子账户的地址，而 DREP 方案中，不需要生成子私钥，通过 Private Seed 即可将主账户与子账户的地址联系起来，存储大小明显减少，并减少计算开销。

除此之外，DREP 采用安全多方计算、环签名等手段将用户 ID 携带信息进行保护，将数据滥用与泄露的风险降到最低。

### 3.2.2 Zooko 三角的突破

Zooko 三角[18]是一直是网络中命名系统的三个理想性质的三难选择困境。

- 安全：当你查找一个名字时，你能够得到正确的结果，而不是一个假名。
- 去中心化：没有中心化权威机构控制所有的名字。
- 可理解的：名字是人们可以记住的，而不是某一长串随机的字符。

DREP ID 的 Alias 身份系统可以突破 Zooko 三角的限制。用户将在安全去中心化环境中产生一个可以理解的别名/昵称以代表自身 ID，方便记忆的同时补充了自身声誉形象。

### 3.2.3 通用性

DREP ID 通过 DREP SDK 达成去中心化登录，兼具第三方登录与自主身份之长，支持大量应用以 DREP ID 的身份登录，同时自主控制发送信息。另外，DREP ID 兼容 BTC、ETH、EOS 等各区块链架构，不受应用所处区块链局限。

---

[17] Dworkin, Morris J. *SHA-3 standard: Permutation-based hash and extendable-output functions*. No. Federal Inf. Process. Stds.(NIST FIPS)-202. 2015.

[18] https://web.archive.org/web/20011020191610/http://zooko.com/distnames.html

### 3.2.4 便利性

DREP ID 通过客户端对接多种资产，可打通资产壁垒，方便跨链转账。同时 DREP 客户端将集成各应用平台，支持多种资产支付与兑换。用户亦可将身份数据存储于 DREP ID 上，在应用需要个人身份信息时自主选择信息传递到应用端。

### 3.2.5 唯一性

DREP ID 由于去中心化，不可能限制用户注册，也无法强迫用户进行 KYC。但由于 ID 声誉形象越丰富越有利的原则：将自身不同应用中的账户以子账户形式绑定在 ID 上，将更加有利于自身被信任与获得优势，用户使用唯一 ID 比分散多个 ID 将更加可信。这将激励用户产生 “第二身份”。

## 3.3 DREP 声誉协议

声誉系统将配合 DREP 的 DREP ID 系统，提供 ID 的长期持有价值，解决如何提升客户/用户忠诚度，做出真正有激励的积分系统，如何获取线上的征信数据，获取精准的用户画像和高质量的用户等痼疾，实现 B2B2C。

### 3.3.1 声誉系统的架构

DREP 声誉系统包括通用声誉协议、声誉管道接口、声誉上链与算法库、声誉奖励获得和声誉账户管理与虚假检测等项目，构成完整生态闭环，从而将用户的行为与声誉挂钩，综合多方声誉评价，进行声誉变化的即时结算并反馈给用户。

**通用声誉协议**

- 将不同平台上用户的声誉数据及数据变化记录在区块链上，达成不可篡改的声誉上链。
- 打破已有壁垒，进行用户行为的跨链，形成对声誉数据的实时同步。
- 将不同平台的用户声誉集中在用户的 did 之中，形成完整的用户声誉画像。

**声誉管道**

采用智能管道技术，避开智能合约的巨大消耗，不影响区块链性能的前提下大大提升数据处理能力，从而实现对用户声誉变化的实时结算。

**声誉算法库**

DApp面向的行业各不相同，即使是同一个行业内，DApp 也都会有很多的差异，因此用同一个算法来计算声誉值是不可能也不科学的。DREP 系统中，默认的声誉算法是随时间推移不断减少的历史累计+现在获得值，并将声誉值的计算方法开放给 DApp，根据自己的业务模

型及特点做针对性的调整。同时，DREP 系统会根据几个大类的行业推出各自典型的算法模板，供 DApps 选择：

- 电商
- 在线问答
- 博客
- 论坛
- 娱乐（视频，音乐，游戏等）

此外，我们还将开发第三方算法库的算法平台，鼓励开发者及 DApps 开发并开源自己的算法。对于第三方算法库引入，DREP 也将会给予经济激励。

**声誉奖励**

DREP 认为，Reputation 同样可以成为一种财富，但其价值尚未得到释放。所以设计了基于 Reputation 的奖励。奖励通过之前对用户行为的采集、上链与计算的结果，给予 DREP 作为奖励，同时也可以选择相应平台的优惠。

**声誉账户管理与虚假检测**

DREP 的声誉体系通过 DREP ID 连接每一个 DApp 平台，从而连接了每一个拥有的声誉值的用户。DREP 会对生态进行严格的声誉值账户管理：

- 同一DApp 上，用户只能在唯一的公钥地址上积累声誉值，并存储于区块链网络。
- DREP支持各个 DApp 对用户进行精准分类、筛选、授权，并提供定制化服务或进行特定场景的经济激励。
- 隐私管理：用户对于声誉值具有隐私管理权，用户可选择是否授权读取其他 DRApp 上的声誉值，也可授权其个人声誉值是否对其他用户可见。

虚假账号鉴别为 DREP 持续研究和改进的模块。因为随着互联网平台的演进，区块链、物联网等技术与传统互联网平台的结合，虚假账号鉴别机制也应当随之改进。

DREP 通过声誉值识别阈、 防 Sybil 攻击机制与第三方KYC（身份信息验证）平台联动等方式排除虚假账号，让用户自发维护声誉与形象。

## 3.3.2 声誉系统的优势

**通用性**

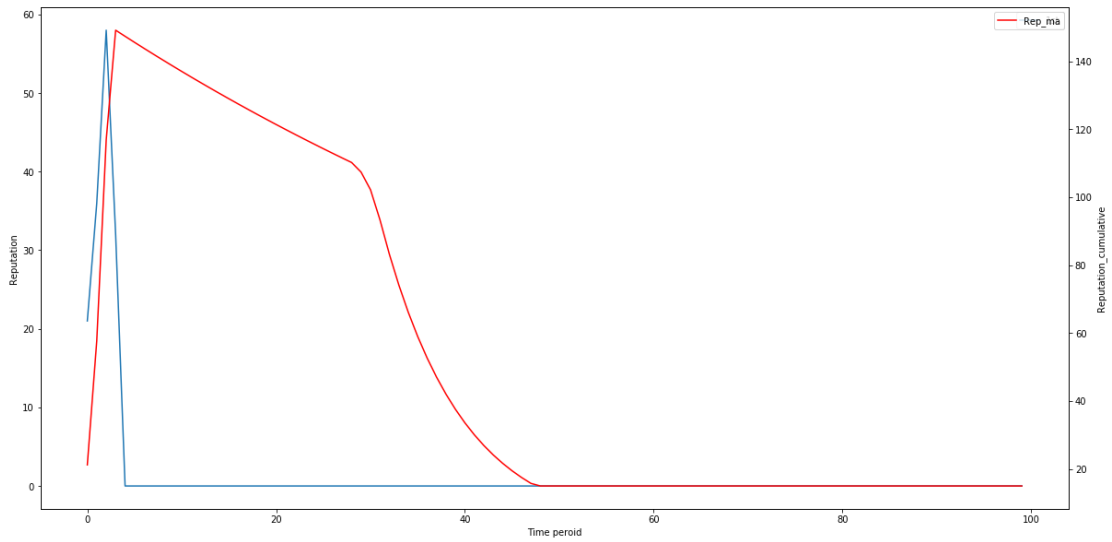
声誉协议并非为单一平台设计的协议，而是能够跨平台打通原有数据瓶颈，对于不同行业也有相应的模板以供应用。只需要根据本行业/本平台进行细节的调整，就能得到平台用户的忠诚度，其平台用户亦可在自主范围内进行数据共享，降低数据获取成本。

**时效性**

DREP 对用户行为产生的声誉具有时效性，即距离现在时间越远的行为对累计声誉影响越小，鼓励提高 DAU，提高用户对平台的粘度。

声誉时效性通过声誉管道，每 1 天或即时反映在用户声誉变化上。

声誉时效性的计算根据 DREP 开发部分提出的声誉衰减获取模型进行，如下图所示，某用户仅在第 1-3 天使用应用，从第 4 天起不再使用该应用，产生的声誉变化（蓝线为获得声誉，红线为累计声誉）：




声誉早期衰减较慢，后期则迅速收敛到一个较低的基础值。用户下次再使用应用，将不再从 0 开始。

**闭环性**

DREP 声誉协议不仅对 B 端具有重要意义，C 端用户也可以从声誉获得实惠。通过声誉汇集换取相应的优惠，进一步促进使用与消费，形成生态闭环。

## 3.3.3 声誉系统对 ID 的补充与增强

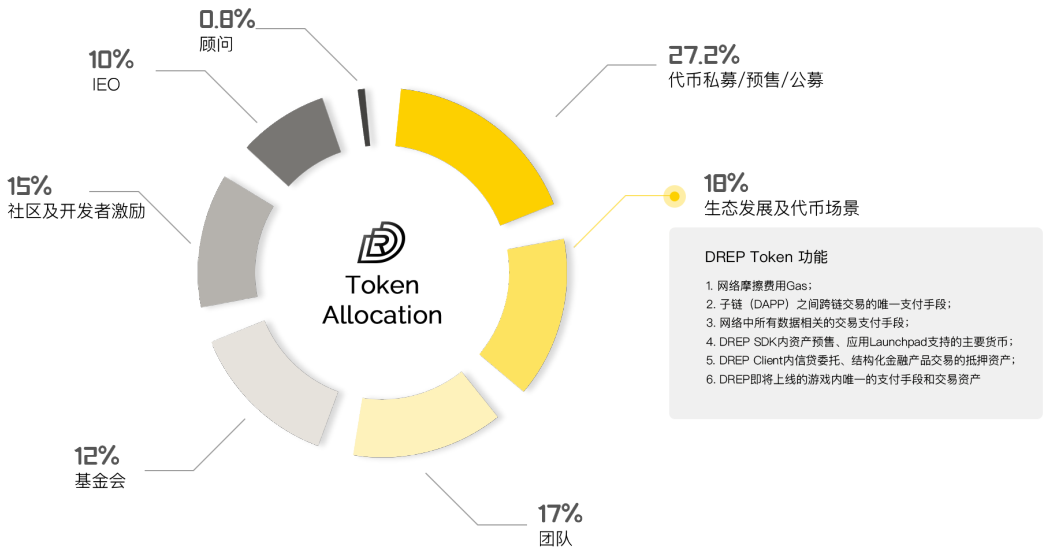
DREP 的声誉协议并非仅对积分体系进行补充、拓展或者替代，在不同应用中产生的生态，将最终汇总成用户声誉形象。

对于真正的精准推荐、精准营销而言，单纯获得用户在某个应用上的活跃信息不足以刻画出完整的用户形象与兴趣。但通过汇总声誉形象，则可以通过大数据等方法找出用户的兴趣点或者符合用户习惯的用户类型，进而深层次满足用户需求，同时避免用户隐私方面指控。

# DREP 代币经济模型

**DREP 总共发行 10 亿枚代币，代币的分配方案如下：**

- 生态发展及代币场景：18%
- 社区及开发者激励：15%
- 代币私募/预售/公募：27.2%
- IEO：10%
- 团队：17%
- 基金会：12%
- 顾问：0.8%




**DREP 代币在 DREP 生态系统中的使用场景主要为：**

- 网络摩擦费用 Gas；
- 子链（DApp）之间跨链交易的唯一支付手段；
- 网络中所有数据相关的交易支付手段；
- DREP SDK 内资产预售、应用 Launchpad 支持的主要货币；
- DREP Client 内信贷委托、结构化金融产品交易的抵押资产；
- DREP 即将上线的游戏内唯一的支付手段和交易资产。