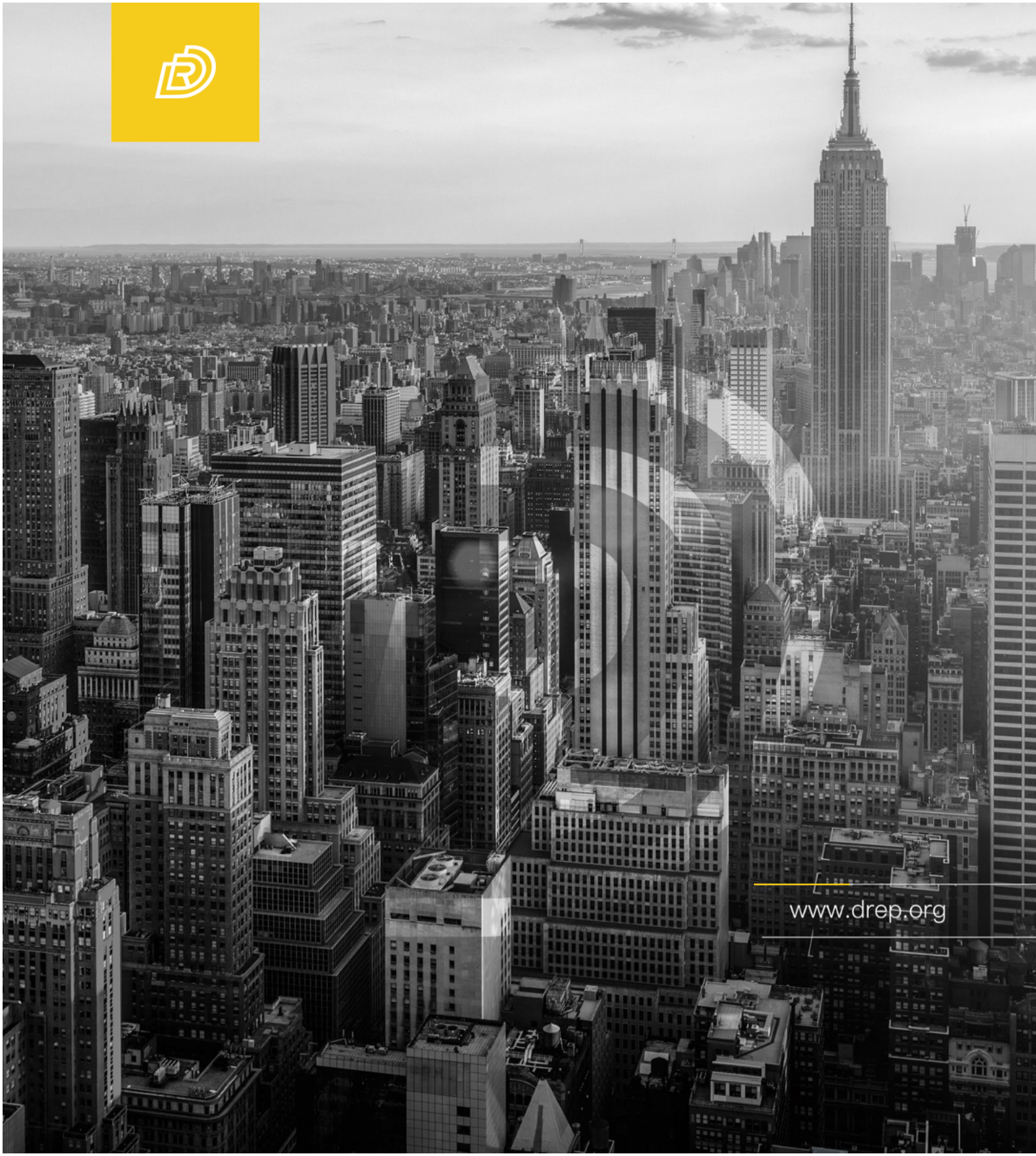


WHITEPAPER

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.

Abstract

If the commercialization of the internet is because it connects information. Then we can say that the reason why blockchain could rise above the Internet and the Internet of Things (IoT) is that it breaks the data barrier, connecting everything. DREP is committed to building “connectors” and “toolkits" on blockchain technology, providing solutions that combine ease of use, flexibility and frictionless integration.

Current blockchain adoption is still in segregation and data are still in silos. Both general public chains and vertical industry chains establish a closed ecological system in order to maximize competitive advantage. As a result, dApps (decentralized applications) have to develop independent versions for different public chains in order to reach more users, resulting in segregated user-and data-base. To face this issue, DREP priorities decentralized ID, cross-chain structure and DREP SDK to serve as a “connector”, supporting multi-public-chain asset versions with one-click, cross-platform data integration and privacy protection in data sharing based on homomorphic encryption.

As blockchain moving from research labs towards real-world applications and mass adoption, enterprises, more often than not, lack enough blockchain knowledge to find out potential usages of this technology in the existing operation. At this stage, be it infrastructure layer or application layer, a light, high-quality, productized solutions is much needed to quickly penetrate the market and solve pain points of business fragmentation, hence acquiring a desired technological input-output ratio and maximizing user experience. In this respect, DREP, functioning as a “toolkit”, adopts a customized dual-layer architecture and advanced API and Plug-in support as well as DREP SDK catering to differing verticals.

In short, DREP’s mission statement is,

- not just tied to high concurrency, but to make it no longer a bottleneck limiting businesses;
- not just tied to customer-oriented service, but to allow B-end and C-end users use blockchain services in a frictionless manner;
- not just tied to commercialization, but to connect every isolated database.

DREP Definition

DREP is committed to building “connectors” and "toolkits" based on blockchain technology, providing solutions that combine ease of use, flexibility and frictionless integration. Based on DREP Chain, DREP ID, DREP Reputation Protocol and DREP SDK, DREP aims to build an open data ecosystem on chain, disrupting the status quo of segregated users and data on multiple chains.

So far, numerous projects have come to the market, providing solutions in scalability, security and privacy. However, their blockchain infrastructure can only serve a very small number of applications which are limited in scale and category. On the other hand, large-scale enterprises rarely see mass adoption of blockchain technology, making it more difficult to bring in new users to the space.

DREP, for those very reasons, strives to tackle three particular issues:

- Insufficient performance of public chain and poor developer experience
- Segregated public chain ecosystem and small user base on blockchain
- A mismatch between blockchain technology and enterprises’ needs

DREP mainly provides the following technical solutions:

- The DREP Chain is a high-performance public chain fully developed by the DREP team. It is compatible with Smart Contracts in the EVM and WASM format with a dual-layer structure constituting of a root chain and sub-chains.
- The Smart Pipeline innovatively proposed by the DREP team is a "pipeline" for data transmission and for transferring data between the blockchain virtual machine and external applications. It is able to achieve high efficiency, zero gas consumption and strong scalability without affecting security. These realistic needs were not solved with the use of Smart Contract.
- DREP adopts a Schnorr multi-signature algorithm based on Secp256k1 to improve network efficiency and reduce transmission overhead.
- To achieve data connectivity and privacy protection, DREP has designed a decentralized ID system based on HMAC (Hash Message Authentication Code) algorithm, forming a dual-layer system of master ID and multiple sub-IDs. DREP Client allows users to manage data and assets on centralized and decentralized platforms at one go.
- To enhance data privacy protection, DREP uses homomorphic encryption to process information that users identify as private.
- To provide long-term holding value of DREP DID, DREP launched a reputation system. This consists of a general reputation protocol, reputation pipeline interface, reputation data on-chain and algorithm library, reputation incentive mechanism, reputation account management and fake account identification mechanism, etc.
- To lower the threshold of technical usage and the cost of learning, DREP has developed API, Plug-ins and SDKs for a number of differing verticals. With these toolkits, DApp R&D teams are able to release multi-public-chain asset versions, built-in wallets and asset trading platforms with one-click. Based on DREP ID, DApp R&D teams are also capable

of acquiring more public chain users, transforming various digital asset holders into application users and creating Super DApps.

- DREP code style is to Service-oriented programming, similar to Java's Spring container development. In most blockchain project code, the coupling between the modules is more serious. Using this approach, DREP allows the modules to be fully decoupled and the code can be easily refactored with a clearer logic.

Before the DREP Mainnet is officially released, there will be 4 iterations of DREP Mainnet, representing four important milestones of the development team. It also represents that DREP constantly explores pain point solutions and optimize user experience in the process of communication with the cooperative enterprises and product portfolio iteration. DREP's 4 Testnets are named after Darwin, Riemann, Euler and Planck, to pay tribute to the great contributions of the four scientists in the process of human development, while symbolizing that the DREP team is on a continuous endeavor to technology development and commercial application.

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

DREP Solutions

2.1 Insufficient performance of public chain, poor developer experience

Transactions Per Second (TPS) is one of the major limitations for public chain adoption. Third party payment solution Paypal currently boasts 100 TPS whilst Visa is able to process up to 2000. On the contrary, Bitcoin and Ethereum can only process 10 TPS, which not only constrains blockchain payments but also makes it harder for developers to create DApps suitable for mass adoption.

The continuous development of DApps has led to the amount of on-chain data being processed through them greatly increased. For example, EOS's RAM is already 62% in use with the usage ratio and resource cost increasing consistently over time, making it more difficult for public chain platforms to grow. In addition, given the issues with concurrency, it is impossible to rely solely on protocol layer Smart Contracts to record DApp data.

There exists an Impossible Blockchain Triangle that decentralization, scalability, and security cannot all be satisfied. This means public chains cannot improve TPS without sacrificing decentralization or security. DREP has proposed an alternative method to improve scalability called the 'Smart Pipeline.' Similar to a Layer 2 solution, it can improve data processing capacities in batches, provide customized developer tools and therefore break the bottleneck of public chain scalability.

2.1.1 DREP Smart Pipeline improves data processing capacities in batches

The Smart Pipeline is an innovative blockchain application model proposed by the DREP team. It is able to achieve high efficiency, zero gas consumption and strong scalability without affecting security. These realistic needs were not solved with the use of Smart Contracts.

Whilst Smart Contracts are widely used on platforms such as Ethereum, the data capacity, gas consumption, and lack of active calling functions are criticized by developers; this effectively limits the development of large-scale DApps.

The DREP Smart Pipeline is a "pipeline" for data transmission and for transferring data between the blockchain virtual machine and external applications. The blockchain client transmits real-time data to an external application through the Smart Pipeline and the external application executes the result before passing the Smart Pipeline and return data to the blockchain client in real time.

Smart Pipelines can be inserted into every step of process and the corresponding code can be executed according to the position of the selected inserter to improve execution efficiency.

The advantages of Smart Pipeline:

- **"Smarter":** After the Smart Pipeline is deployed on-chain, it can automatically trigger according to the conditions detailed. Compared with Smart Contracts, more conditions can be considered and the execution process can be made more difficult to interfere with; this is conducive to the execution of complex transactions.

- **Zero gas consumption:** When an application using Smart Pipelines executes a transaction, no gas is needed. Zero gas consumption does not mean zero responsibility, however, and all Smart Pipelines running code require open source supervision. Moreover, the computing resource body that the Smart Pipeline directs to is not only found on the corresponding sub-chain, but on the Smart Pipeline code. Thus, even if there is a loophole, it will not affect the performance of the corresponding sub-chain.
- **No limitation in programming language**: Smart Pipeline uses the WASM virtual machine to execute transactions. Users can write code in different programming languages and then convert to WASM. As WASM continues to improve, the types of languages supported will gradually increase, and the code efficiency will also be improved without affecting execution on the blockchain.
- **Meets the needs of complex applications**: Smart Pipeline applications are not limited by gas and can be supported on blockchains to facilitate more complex logic. Blockchains with Smart Pipeline can interact with other applications or services to meet the needs of large, complex applications, hence allowing for the building of applications that are not supported by existing blockchains.

2.1.2 DREP dual-layer architecture and customizable sub-chain

The DREP Chain takes form as a dual-layer structure constituting of the main chain and sub-chain to improve scalability and enhance the efficiency of the blockchain infrastructure without affecting security or decentralization. In DREP's open source Testnet, the DREP Chain TPS exceeded 12,000 at peak during an open test on January 8th, 2019.

Test environment conditions were:

- 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

The DREP main chain and the sub-chain can independently handle different transactions, allowing for multiple consensus mechanisms to coexist with different data storage, improving concurrency, and providing compatible support for access in different applications. Therefore, whether used in a blockchain application, traditional enterprise or docking platform, the corresponding sub-chain can be customized to reduce the barrier to entry.

2.1.3 DREP improved consensus mechanism

PBFT is a safe and efficient consensus mechanism which has been applied to consortium chains such as hyperledger, but the existing PBFT consensus mechanism does not meet the needs of the public chain in terms of consensus efficiency. DREP enhances PBFT through using a Schnorr multi-signature algorithm, integrating a large number of signatures into one signature, improving DREP

Chain efficiency in storage and network transmission, and reducing network transmission overhead. Thus, PBFT can be applied to the DREP Chain system.

2.1.4 DREP developer tools

DREP will provide a series of development resources for DApp development and sub-chain customized development, including a Docker, IDE and other upper-level tools as well as console and other underlying services. In addition, test tools such as browsers, faucets, testnets, etc., will be created to assist DREP developers.

DREP Docker has the advantages of quick set-up, easy installation and deployment; DREP Console has programmable and interactive features, supports script operation, and is beneficial for developers; RPC interface and JS library can also be used for multiple functions such as node access.

2.2 Separated public chain ecosystem and small blockchain user base

The biggest competition in blockchain lies in the “main chain”; each main chain strives to become the flagship product in blockchain infrastructure, and hence secure the position of ‘Apple’ or ‘Microsoft' in the technology sector. As a result, operability restrictions are common between various public chains varying from infrastructure to DApps and resulting in separated user bases, such as with ETH and EOS users. This inevitably leads to "Prisoner's Dilemma" in public chain development.

DREP based DREP ID, aims to assimilate user accounts scattered across various public chains and further expand this model to traditional platforms, letting more users access the blockchain frictionless and thus resolving the problem of small user base, promoting adoption and encouraging developers to remove barriers between various public chains.

2.2.1 DREP ID connects digital assets

DREP ID integrates all types of cryptocurrencies through the DREP Client, giving users access to one-stop account management. In addition, binding different platform addresses to DREP ID allows cross-platform transfer by way of cross-chain interoperation.

Such functionality is not just confined to blockchain. For traditional/centralized platforms within the DREP network, cross-platform management is also available through DREP ID to achieve asset and data integration, encryption of information, etc. without interfering with the existing numerical systems, integral system, economic system or other aspects of the original platform, forming an interconnected and decentralized ecosystem.

In this way, DREP ID is able to support cross-chain Super DApps, allowing DApp developers and users to transfer mainstream currencies freely without suffering from infrastructure restrictions, and freely trade tokens on Decentralized Exchanges. As a result, user experience would be improved, user bases would be expanded and unnecessary development be reduced.

2.2.2 DREP ID connects user information

Blockchain’s barrier to entry and usage partly lies in incomprehensible 20+ digit public key addresses. Only a small number of public chains, such as EOS, have addressed this. Despite that,

each address registered on EOS still requires payment. Worse still, when addresses are plenty, memorization becomes a problem and the price skyrockets.

DREP users are able to use an alias which is understandable and able to be remembered; this lowers the threshold to blockchain usage. Also, managing various addresses under one name results in gas reduction and aliases on DREP do not have to deal with 20+ digit public key address but a nickname for the account, which DREP has already stored on blockchain.

For existing accounts, recording specific and complex information becomes unnecessary when linking with DREP ID. After DREP ID generates a new sub-account, addresses recording also becomes unnecessary. This is convenient for end users as the Alias serves as a users' DREP ID marker, connecting various sub-accounts through DREP Reputation Protocol, contributing to a users' credibility and raising awareness to their "second identity" ——DREP ID.

2.2.3 DREP ID protects user privacy

Many centralized platforms analyze and resell users' data without obtaining their consent. Some even trick users into purchasing that relevant information. With DREP ID, users have the option to disclose their data. In terms of users' privacy, third parties have to pay to collect such personal information. As a result, users can receive DREP tokens as rewards and third parties can obtain more accurate data including metrics such as user's reputation value and lower acquisition cost of data.

When logging into centralized platforms, servers have the access to info such as: users' names, users' accounts and more. When user logins with associated accounts, platforms are also able to profile users despite not giving notice. DREP ID, combining with third party logging and in avoiding privacy intrusion, gives users the right to choose what information platforms are able to acquire, and in which ways they can login. As a result, users do not have to remember multitudes of accounts and passwords whilst protecting their privacy.

2.3 A mismatch between blockchain technology and enterprises' needs

Blockchain is highly anticipated as a way to innovate production. However, due to its limitations, low efficiency and lack of talent to connect blockchain and enterprise, progress in this area is slow.

DREP believes blockchain developers ought not to "close the door" and predict market needs, but look more closely at the market and understand the real needs for clients and users. After learning the pain points and difficulties in blockchain development, one could develop kits for easy integration into a number of differing verticals.

Based on market research, DREP offers two solutions: one is to upgrade DREP advanced technology solutions to allow API and Plug-in support, thus lowering blockchain learning costs, development difficulty and complexity on the application/enterprise side. The other is to develop customized SDK's for vertical domains, solving specific problems in development and forming a complete vertical domain technology solution.

2.3.1 DREP API and Plug-in, simpler and easier use

DREP API is adaptive to different languages, making it easier for centralized platforms to decentralize.

DREP Plug-in aims to satisfy more accurate and complex needs and is conducive to vertical domain development.
Advantages of DREP API and Plug-in:

- Highly-targeted development without complete comprehension of blockchain, making it easier to enrich functionality.
- Supporting co-development and making it easier to adjust or modify during the development process.
- Converting practical problems to blockchain solutions directly, making it easier to use.

2.3.2 DREP SDK, aimed at vertical industries

DREP SDK supports DApps of all kinds. With DREP SDK, DApp R&D teams are able to release multi-public-chain asset versions, built-in wallets and asset trading platforms with one-click. Based on DREP ID, DApp R&D teams are also capable of acquiring more public chain users, transforming various digital asset holders into application users and creating Super DApps.

Super DApps: DApps are not confined to certain public chains, but connect various digital assets, making it possible for all users to pay, transfer, lend and conduct other economic activities. At the same time, users of traditional platforms are able to apply for blockchain DApp versions, greatly lowering user education costs.

DREP SDK for blockchain gaming including but not limited to:

- Gaming accounts: Highlights cross-chain DREP ID, removing current segregated user base;
- Payment & trading: Highlights built-in payment and trading engine, improving the digital asset exchange experience;
- Digital operation: Highlights data visualization, transparency and configurability within gaming operations.

DREP Technology Framework

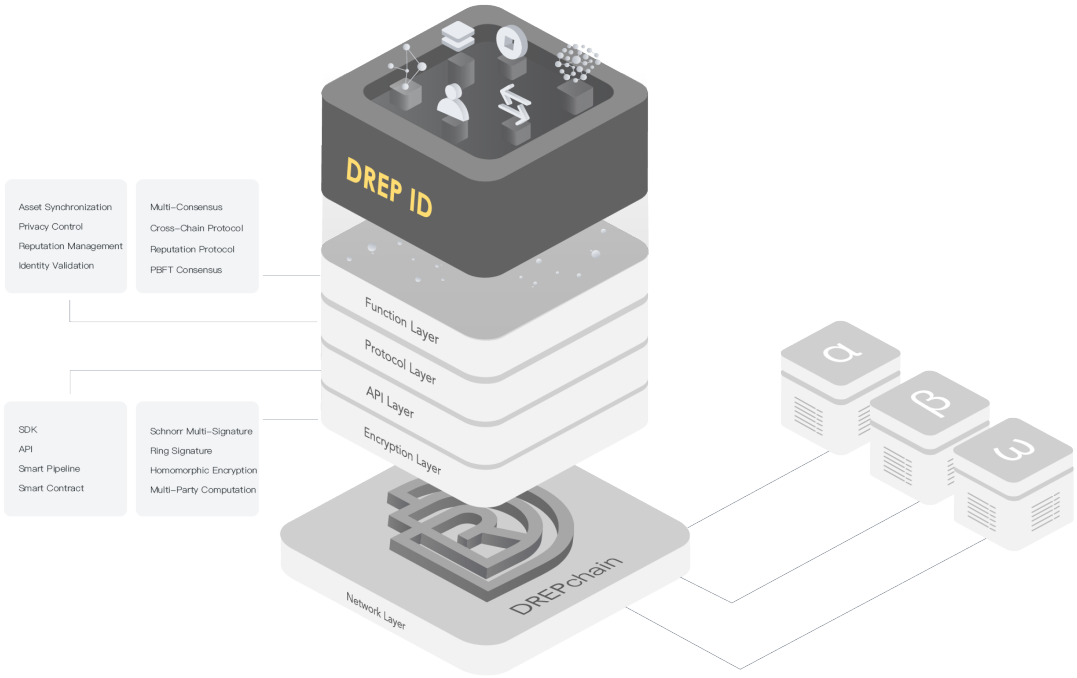
3.1 DREP public chain

The DREP Chain is a high-performance public chain fully developed by the DREP team, which is compatible with Smart Contracts in EVM and WASM format with a dual-layer structure constituting of a root chain and sub-chains. The root chain is mainly responsible for data sync to the sub-chains and DREP token transactions, and sub-chains make it easier for enterprises to develop DApps and their own blockchain ecosystems. This allows enterprises to independently distribute tokens, deploy Smart Contracts and Smart Pipelines, exchange assets and share reputation values across multi-chains.

The DREP Chain prioritizes efficiency when it comes to consensus selection. This explains why during the DREP Testnet 1.0, an improved PBFT was deployed as the consensus mechanism for sub and root chains. In the future, root chains will gradually adopt a POS mechanism with reputation.

DREP, evolved out of the traditional PBFT consensus mechanism, introduces PBFT based on multi-party signature to improve efficiency not only reflected in TPS, but also in the process of storage and network transmission. With the original PBFT protocol, participants had to send information signatures to the Leader, then the Leader integrated signatures into the block header. With multiple signatures, the size of block header can be increased. DREP deploys Schnorr multi-party signature algorithm supported by a Secp256k1 elliptic curve, resulting in only one signature being generated, this greatly reduces the signature length and thereby reduces the size of block header and the cost of storage as well as network transmission overhead.

DREP technical structure is as follows:



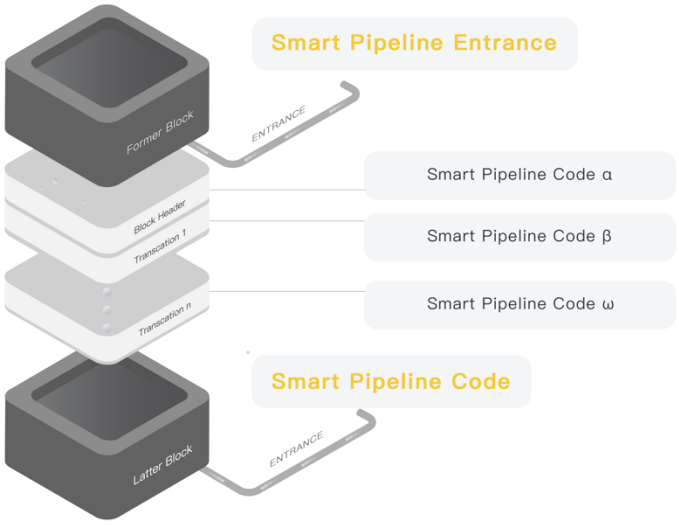
3.1.1 DREP Smart Pipeline

DREP proposes the concept of Smart Pipelines to improve data processing and transfers of data between blockchain virtual machines and external applications. Smart Pipeline, when compared with Smart Contract which is already widely used on platforms like Ethereum, boasts advantages of high efficiency, strong scalability and zero gas consumption.

Problems of Smart Contract lie in:

- Block package has very limited maximum data capacity. For instance, the ETH model, current maximum Gas in a single block is 3,141,592 Gas; this means if attached data fails to reach 1M, a jam may occur. This means DApps cannot cope with large amount of data for fear of jamming.
- The cost of reading, writing, and calculating Smart Contracts is exorbitant. As a result, developers are reluctant to use algorithms that are very popular on traditional platforms but consume large amount of gas on blockchain, limiting DApp design.
- There is no active calling function, which means Smart Contract cannot automatically perform complex tasks such as fixed time tasks that require external script support.

A sketch of the Smart Pipeline is shown below:



When a blockchain produces a block, transactions are conducted in the virtual machine in turn. Smart Pipelines can be inserted before or after each execution. Smart Pipeline functions as breakpoint and clients can activate a part of pipeline/breakpoint in accordance with their needs. When a client executes an activated Smart Pipeline/breakpoint, a stop-the-world process would automatically be triggered, and real-time data transmitted to external application through Smart Pipeline. External applications are responsible for data processing, and after processing, the result is sent back to client on blockchain via Smart Pipeline. From there, the client stores data into the database, thereby completing data uplink to blockchain. Such processes avoid the drawbacks of a large amounts of data processing in virtual machine. Transmission does not hinder operation

efficiency, instead, it improves data processing due to the fact that Smart Pipeline is deeply optimized by DREP.

DREP Smart Pipeline application consists of a WASM instruction set, which is distributed throughout the blockchain. Different sub-chains can also choose different applications to execute or be executed by self-written and verified applications.

3.1.2 DREP cross-chain protocol

The DREP cross-chain protocol transcends traditional thinking about cross-chain transactions being only for transferring assets as it also synchronizes and migrates behavioral data related to personal identities such as reputation (credit rating/loyalty), and then secures it through homomorphic encryption.

DREP adopts both isomorphic and heterogeneous cross-chain solutions to cater for different needs and to cope with performance and cost balancing within different structures:

- **Isomorphic cross-chain:** DREP main chain and sub-chains are connected by a frictionless isomorphic cross-chain protocol; this allows users to learn real-time changes among cross-chain platforms through wallets.

- **Heterogeneous cross-chain:** Distributed private key control technology connects chains outside the DREP system including traditional platforms to the DREP ecosystem in order to achieve a secure heterogeneous cross-chain, extending reputation protocol for multiple platforms.

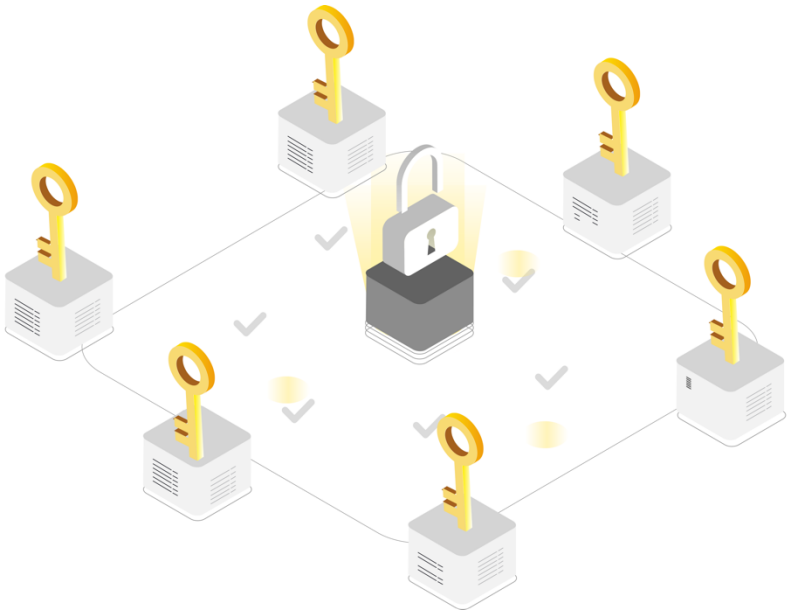
Based on isomorphic and heterogeneous cross-chain technologies, token assets and reputation data on different DApps are integrated to the main account, forming a multi-level and vivid user reputation profile.

In addition, DREP plans to “reputationize” partners’ user behavior, expanding reputation to different systems in accordance with cross-domain security control requirements, and enabling reputation beyond blockchain, thus forming an extensive reputation ecosystem.

Distributed private key control

Distributed private key control utilizes decentralized technology to control cross-chain assets with multiple private keys. The original holder still has ownership, but one single private key cannot withdraw assets. If the holders want to withdraw assets, they need to apply with the corresponding chains and obtain enough private keys.

For example: user Alice wants to convert one token from one chain to another. A number of nodes (shards/super-representative committees) across chains maintain one multi-signed account on the original chain, they allocate private keys and then separately control them, so that any single node cannot obtain this token from the original chain without enough private keys - in which case it is possible.



When Alice deposits one token to a multi-signed account controlled by DREP, one token in DREP is equivalent to a synchronously released deposit token, which can be traded with another node in DREP via tokens in different chains. When Alice wants to withdraw the ownership of one token in original chain, she needs to lock her remaining tokens in DREP, and then release the same amount of tokens as owned on the original chain.

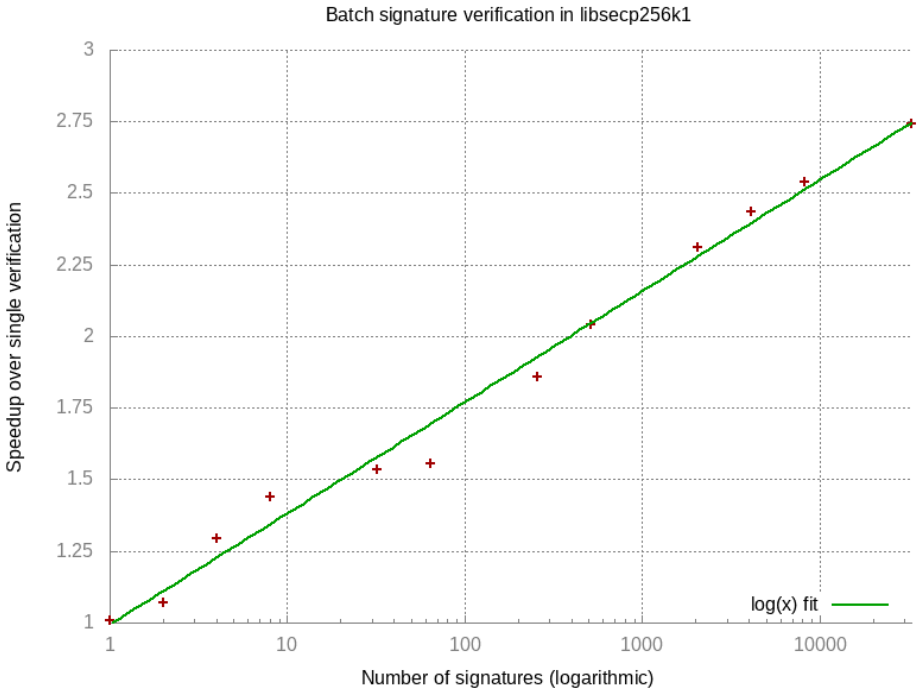
The distributed private key control process is more secure, and supports Smart Contracts, including multi-currency complex contract. This is the case regardless of whether the original chain supports Smart Contracts or not in that it distributes tokens across chains.

3.1.3 DREP privacy protection

Schnorr multi-party signature

DREP introduces the PBFT mechanism which is based on multi-party signature. The traditional PBFT protocol requires participants to send information signatures to the Leader, and then Leader integrates signatures into the block header. However, with multiple signatures, the size of block header would be increased and affect network transmission efficiency. While DREP deploys Schnorr multi-party signature algorithm based on the Secp256k1 elliptic curve, significantly improving blockchain efficiency.

Test results of Schnorr multi-party signature performance in BIP-Schnorr signature are as follows:



Schnorr multi-party signature, differing from other signature forms, only generates one signature in the end. This greatly reduces signature length and block header size, in turn lowering the cost of storage and network transmission overhead.

Schnorr multi-party signature is also conducive to privacy protection when future privacy transactions need to be enhanced.

Homomorphic encryption and privacy protection

During the process of DREP Chain operations, it is inevitable to pass information to third parties - such as internal Smart Pipelines and external data sharing, during which process, user privacy leakage may occur, jeopardizing user ID security. To this, DREP adopts homomorphic encryption to protect data privacy when users are processing this private information.

The algorithm uses the Paillier technique based on the encryption problem of computing n-th residual classes of a quadratic integer group.

Where m stands for a message to be encrypted and $m \in (0,n)$, then select random $r \in (0,n)$ via generated key pairing: public key (n,g) and private key (λ,u), compute ciphertext C as $C=g^m r^n \bmod n^2$.

Ciphertext C is both a homomorphic and homomorphic mixed multiplication plaintext, that is

- **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**

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

Therefore, a variety of data processing can be performed after encryption, and the results can be sent back to the user. Users, through private keys, can obtain the same result done by plaintext data processing, making data leakage impossible.

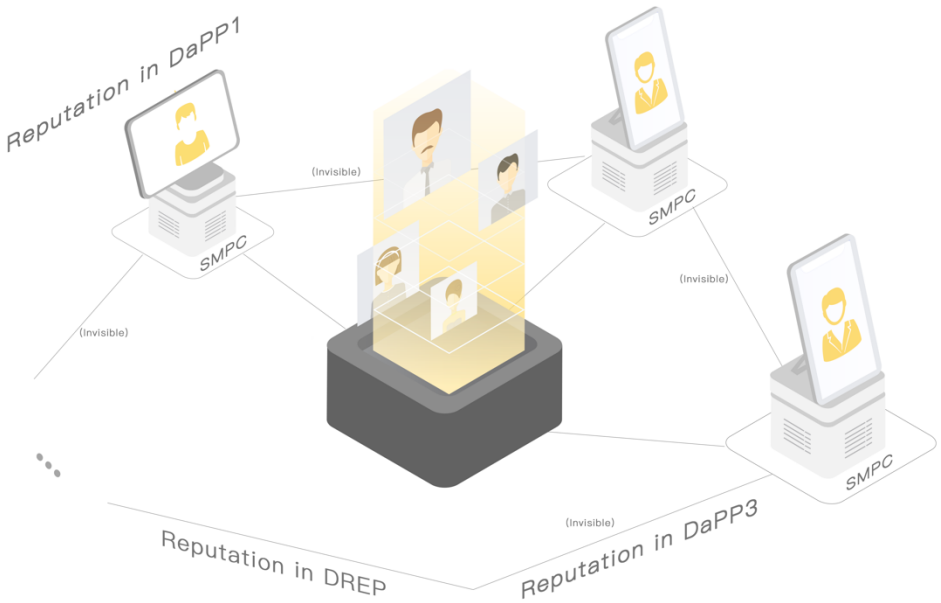
Aside from the above, homomorphic encryption signature availability, when adding a homomorphic signature to content, it is possible to verify misprocessing, spoofing and other forms of misconduct during data processing to ensure data accuracy.

Secure multi-party computation

In the process of distributed private key control and ring signatures involving multiple people sharing private keys, it is necessary to follow the principle of never completely exposing all sensitive information. Therefore, DREP chooses secure multi-party computation to protect data security. Complete information would only be available when it is in use.

Secure multi-party computation deals with the following problem: n individuals respectively hold privacy x1, x2, ... xn, to calculate a specific function y = f (x1, x2, ... xn), while these n individuals do not have access to others' privacy. Given that there are malicious nodes in the real world seeking to obtain other parties' private information, secure multi-party computation protocol denies all participants the right to access any additional information beyond output regardless whether they have malicious intent or not.

DREP conducts secure multi-party calculation through homomorphic encryption, bulletproof and other measures, taking reputation calculation as an example.



DREP deploys secure multi-party computation to encrypt important data within each DApp and DREP platform. Even if data transmission is leaked during transaction, users' original data is safe. Secure multi-party computation also ensures that both parties involved in data transmission are able to encrypt and decrypt data in a safe way. At the same time, users' public key, address and data on each DREP DApp are independent and invisible.

3.1.4 Improvement and optimization

One important reason for DREP developing the DREP Chain lies in the strong coupling with existing blockchain main chains, which currently is not suitable for seamless integration with existing enterprise systems. Additionally, many high-TPS main chains fail to meet existing performance requirements for high concurrent requests transmission.

Structure optimization:

DREP modularizes the various parts of database, network and consensus, then stores these separately in a container. Through middleware, modular calling is performed, resulting in the solution of each module. As well as this, infrastructure is able to automatically implement a series of operations like registration, activation and upgrading of the container by way of middleware. For sub-chain developers, DREP Chain infrastructure code boasts clear logic and easy reconstruction. In addition, DREP has preemptively built a routing and message dispatching mechanism, completely decoupling the network and consensus layers, pushing applicable consensus ranges beyond PBFT, thus facilitating sub-chain independent development consensus.

Virtual machine optimization:

DREP also improved existing EVM to meet DREP chain business needs:

- Increased reputation-related orders in accordance with DREP business
- Upgraded gas pricing, allowing for automatic adjustments in accordance with configuration and demand on each sub-chain
- Re-designed infrastructure database based on business needs

Sub-chain function improvement

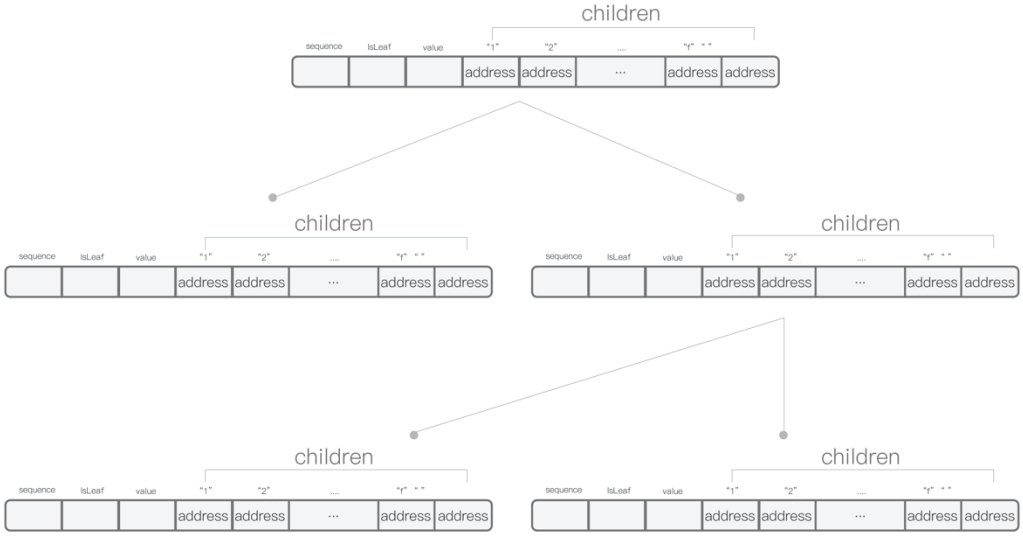
During the process of synchronizing sub-chain data to main chain, if there is a sub-chain data error, a rollback is needed; this is something the original level DB fails to support. Alternatively, DREP, supported by self-developed sub-chain nesting and rollback, is able to solve these problems.

Database optimization

When there are high concurrent requests, the caching mechanism is under great pressure; this means ‘high TPS’ does not necessarily equal high volume of transactions. Additionally, DREP optimizes and improves caches, databases, etc., and uses fine-grained lock inside lRU cache to ensure high performance even when TPS reaches 5,000.

DREP Chain Level DB database utilizes Hash Patricia Trie (Hitton Prefix Tree, hereinafter referred as HPT) technology to preserve changes in users’ account status.

HPT is a K-tree data structure; each node in the tree consists of 4 attributes: Sequence, Value, Children and IsLeaf4. The Value property of the HPT root node preserves Hash value of current database for block verification, ensuring Sequencing property is the only way to get a specific complete Key.



When a user account changes, the database would make corresponding changes to HPT and reflect them. Based on a hexadecimal string key of the user account, the database would conduct a thorough search starting from the root node until a certain leaf node is found; all Sequence attributes on search path are then spliced to obtain a complete key.

Two main advantages of HPT:

- Firstly, the irreversibility and extremely low conflict attribute of the tree structure and Hash algorithm improve the convenience and reliability of database description.
- Secondly, key value design of database and data compression of the prefix tree greatly improve the efficiency of querying and modifying whilst also reducing calculation costs. After each account modification, tree node operations which are equal to the number of HPT depths are able to complete the database update; when modifications are multiple in one transaction, the growth of calculation happening to MPT modification is far below the amount of required account information. With more account information, more MPT calculations could be saved.

Compared with the prefix tree structure used by Ethereum to save account information, DREP HPT unifies and optimizes tree nodes. Instead of adopting Ethereum's null node, leaf node, extension node and branch node, DREP HPT on the one hand, reduces prefix tree height and deep search time, on the other hand, improves HPT query and modification performance.

3.2 DREP ID

DREP ID is the entrance portal to users' digital asset management as well as the digital identity used on DREP and collaborative application platforms. This includes the sum of digital images generated by users on corresponding platforms.

For B-end customers, DREP ID is the entrance portal to user traffic and high-quality data, and a shortcut for cross-chain asset interaction, allowing for payment in multi-currencies/cryptocurrencies.

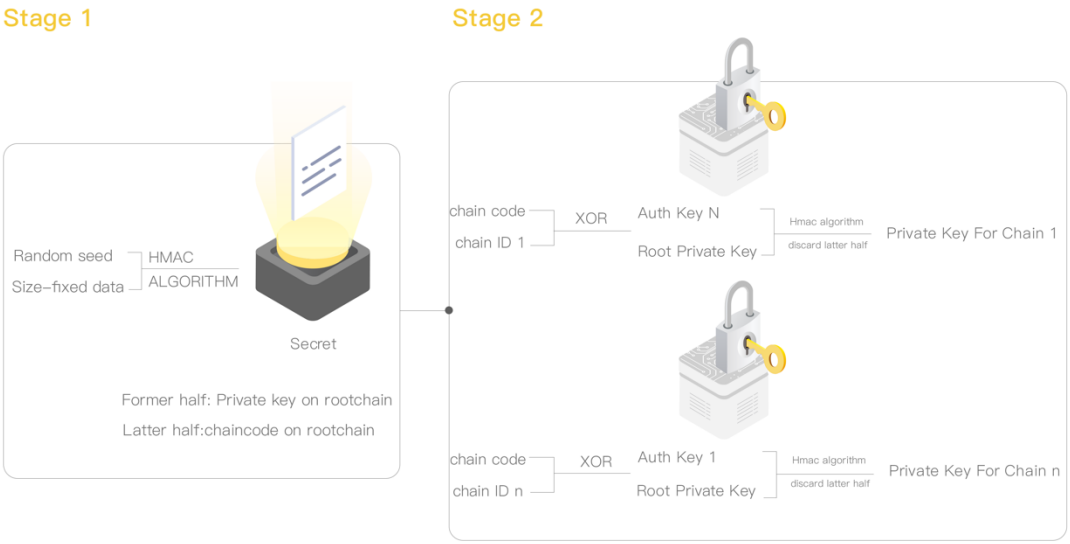
3.2.1 Security

In using the DREP ecosystem, every user has a master account and several sub-accounts. DREP ID serves as a link, connecting reputation data and assets across different applications and building a complete user reputation profile image.

DREP, based on HMAC (Hash Message Authentication Code) algorithm, generates sub-accounts by using the master account.

The formula of HMAC is as follows:

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



K is the master account key, m is the sub-chain ID, both opad and ipad are specific constants. The private key of each sub-account is generated by the private key of the master account and corresponding sub-chain ID, which enables master account to control sub-accounts on each application:

- **Master key control**: when users generate and obtain private keys of sub-chain accounts, private keys, verification codes and sub-chain IDs of the corresponding master account are also required; this guarantees the security of private keys for sub-chain accounts.
- **Unconnectable**: Under asymmetric encryption protection, regardless of main or sub-chain, accounts cannot be reversely connected, making information anonymous on-chain.

DREP HMAC has the following advantages comparing with BTC HD wallet:

- **Variable address length and higher security:** DREP uses SHA3 SHAKE256 (SHAKE=SHA+keccak) to hash public keys, making it possible to set any output address to achieve higher performance and security.

- **Lower calculation cost:** HD wallet needs a large number of sub-private keys to locate sub-account addresses. With DREP, sub-private keys are optional due to Private Seed, which connects master account address with that of the sub-accounts, reducing storage and calculation cost.

In addition, DREP adopts secure multi-party calculation, ring signatures and other measures to protect user ID information, minimizing the risk of data abuse and leakage.

3.2.2 Zooko Triangle breakthrough

The Zooko Triangle has always been a trilemma for three ideal properties of naming network systems.

- Security: When looking for a name, a correct name rather than pseudonym would be presented.
- Decentralization: There is no centralized authority controlling all names.
- Understandable: It's a name, not a long list of random characters that people are unable to remember.

Alias identity system in DREP ID addresses the Zooko Triangle. Users create an understandable alias/nickname in a secure and decentralized environment as representation of their ID, which is easy to remember and conducive to their reputation and profile image.

3.2.3 Universality

DREP ID achieves decentralized logging through the DREP SDK. On the one hand, DREP ID has advantages of third-party logging and self-sovereign identities whilst on the other hand, it supports a large number of applications to log in using DREP ID and controls the information transferred. In addition, DREP ID is compatible with BTC, ETH, EOS and other blockchain structures, and transcends blockchain limitations such as application location.

3.2.4 Convenience

DREP ID connects multiple assets, breaking the asset barriers and facilitating cross-chain transfer. DREP Client integrates into various other applications and platforms to support multi-asset payment and exchange. After users store their identity data using DREP ID, information would be automatically selected and delivered to the application when required.

3.2.5 Uniqueness

DREP ID will not restrict user registration nor will it force users to perform KYC (Know Your Customer) due to decentralization. It is acknowledged that when ID reputation image becomes richer, it can greatly benefit users. Therefore, binding different application accounts to DREP ID in the form of sub-account is beneficial to users' trustworthiness and reputation, because it is more credible to use one unique ID rather than multiple scattered IDs. As a result, users would be motivated to generate a "second identity."

3.3 DREP reputation protocol

The DREP reputation system, along with DREP ID system, endowed ID with long-term value, solves problems like improving customer/user loyalty, making a truly valuable point system, obtaining online credit scores, and acquiring accurate user profile image and high-quality users, greatly assisting B2B2C products.

3.3.1 An overview of the reputation system

The DREP reputation system includes a general reputation protocol, reputation pipeline interface, reputation uplinking to chain and algorithm library, reputation reward acquisition, reputation value account management and fake account identification mechanisms, etc., constituting eco-connection, which links users' behavior with reputation, and conducts real-time reputation settlement, and gives feedback to users based on a comprehensive multi-party reputation evaluation.

General reputation protocol

- Record users' reputation data and data changes across different platforms on blockchain to achieve immutable on-chain reputation modelling.
- Break existing barriers and conduct cross-chain transmission of user behavioral data, forming real-time reputation data synchronization.
- Integrate user reputation amongst different platforms to user's DREP DID, building a complete user reputation profile image.

Reputation pipeline

Reputation Pipeline adopts Smart Pipeline to avoid excessive Smart Contract reliance and improves data processing without affecting the performance of blockchain, thereby bringing real-time user reputation settlement.

Reputation algorithm library

DAPPs cater to various industries whose needs are all very different. Therefore, it is impossible and unscientific to calculate reputation value with a single algorithm. In the DREP system, the default reputation algorithm is the summation of historical increasing/ decreasing + current value over time, and the algorithm for calculating reputation value will be provided for DAPPs, so that they can make customized designs according to their business models and needs. Meanwhile, the DREP system will produce algorithm templates designed for a few major types of industries and provide DAPPs with the following options:

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

In addition, DREP would also develop a third-party algorithm library with the attempt at encouraging developers and DApps to develop their own algorithms and make them open-source. DREP will also have economic incentives for third-party algorithm libraries joining the platform.

Reputation monetizing mechanism

The key concept of DREP is to turn reputation into wealth and unleash its value. That is why DREP has created and designed an incentive module based on reputation. The incentive is given by DREP as a reward through various methods, linkups and by calculating user behavior in accordance with related platform design.

Reputation value account management and fake account identification mechanism

DREP's reputation system connects every user with reputation value by connecting to every DApp platform. DREP maintains strict reputation value account management for users in the ecosystem:

- Users can only accumulate their reputation value on one public key address that will be stored on blockchain within each DApp.
- DREP supports every DApp categorizing, filtering and authorizing their users to provide customized services or personalized economic incentives.
- Privacy management: users have the right to manage their own reputation and choose whether they authorize the platform to access their reputation value on other DApps, as well as whether their personal reputation value can be seen by other users.

Fake account identification is a model for continuous research and improvement. With the evolution of online platforms and the increasing popularity of blockchain technology alongside the Internet of Things, fake account identification mechanisms need to adapt accordingly.

DREP, based on reputation threshold, Sybil attack prevention mechanism and third party KYC identification platform integration, excludes fake accounts, so that users can maintain their reputation and image.

3.3.2 Advantages of reputation system

Universality

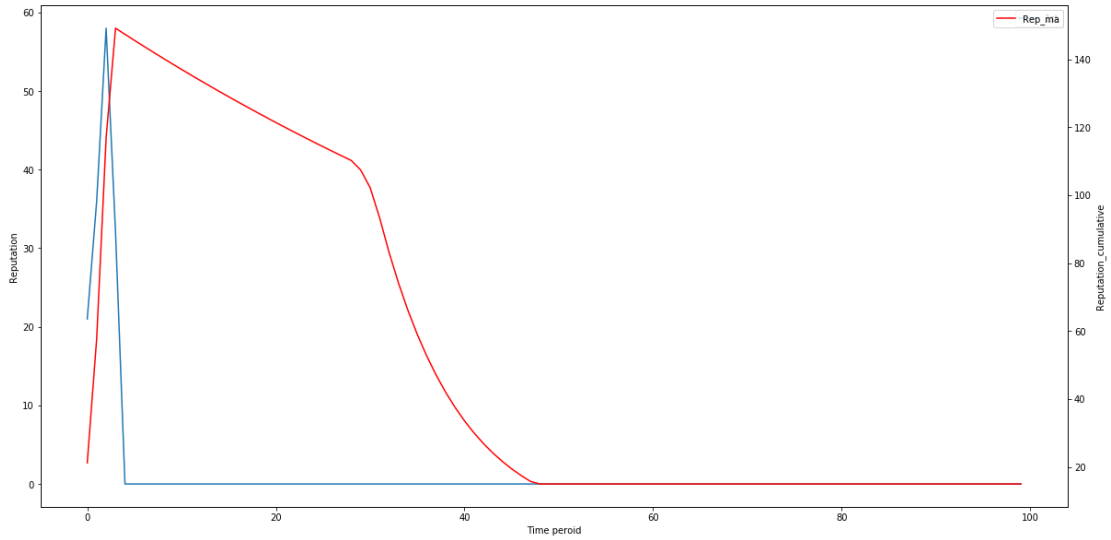
The Reputation protocol is not designed for any single certain platform, but caters to different industries with different templates featuring cross-platform and data integration. It is easier for industry/platforms to obtain users' loyalty by making small adjustments. Moreover, users are allowed to share data as wish, lowering data acquisition cost.

Time-effectiveness

DREP reputation is time-efficient in terms of user behavior, that is, the longer ago something happened, the smaller impact it would have on reputation, thus encouraging DAU, and increasing users' dependence on the platform.

Reputation time-effectiveness, through reputation pipeline, is reflected in the daily or instant changing of user reputation.

The calculation of reputation time-effectiveness is based on the reputation decay acquisition model proposed by DREP dev team. As shown in the following figure, a user stops to use an application after 3 days, resulting in a reputation loss (The line in blue is acquired reputation while the red one is accumulated reputation):



Reputation falls slowly in the early stages and quickly over time. The next time this user activates the same app, it will no longer start from 0.

Comprehensiveness

The DREP reputation protocol is not only of great importance for B-end clients but also beneficial for users. Through reputation collection, it is able to offer customized preferential treatment, further promoting engagement and consumption, thus forming an eco-connection.

3.3.3 Reputation system complements and enhances ID

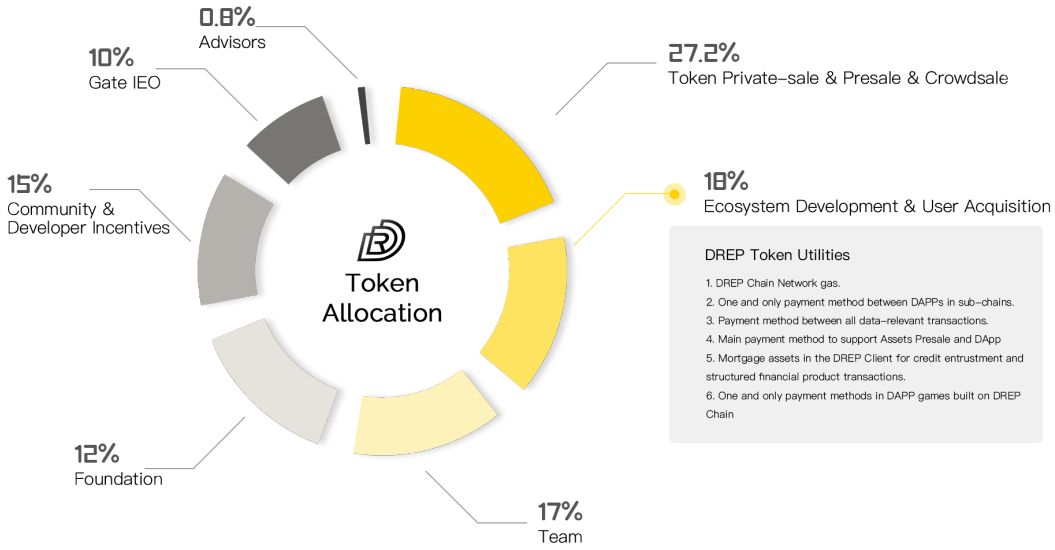
The DREP reputation protocol does more than supplement, enrich and replace traditional point system. The ecosystem of different applications will eventually collectively attribute to users' reputation image.

In terms of targeted recommendation and marketing, information from one application is not enough to portray a user's complete image and interests. While reputation image integration could pinpoint a certain user's interest or the type of users that have a certain habit through big data and other methods, completely satisfying users' needs whilst avoiding privacy infringement.

DREP Tokenomics

DREP issued a total of 1 billion tokens. The distribution plan for tokens is as follows:

- Ecosystem development and utility scenarios: 18%
- Community and developer incentives: 15%
- Token private sale / pre-sale / public offering: 27.2%
- IEO: 10%
- Team: 17%
- Foundation: 12%
- Advisors: 0.8%



The utility scenarios of DREP tokens in the DREP ecosystem mainly include:

- Network Gas;
- The only means of payment for cross-chain transactions between sub-chains (DApps);
- Payment currency for all data relevant transactions in the network;
- Major currency used for presales of assets in the DREP SDK and the application of Launchpad;
- Mortgage assets in the DREP Client for credit commission and structured financial product transactions;
- The only in-game payment method and trading assets in future DREP games.