WHITEPAPER

Connectors and Toolkits on Blockchain

V 2.0.2

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 reason behind the commercialization of the Internet is due to an increase in information connectivity, it can thus be foreseen that Blockchain Technology has the potential to surpass both the Internet and Internet of Things as it possesses the ability to connect the “dots” - linking up isolated islands of information via data cooperation systems. DREP is committed towards building “connectors” and “toolkits” on blockchain technology, providing solutions that promotes the ease of use, flexibility and frictionless integration.

Currently, blockchain adoption suffers from a state of segregation with data silos being huge sources of inefficiencies. Furthermore, it has been observed that both the public and industry chains had established a closed-loop ecosystem to maximize competitive advantages. As a result, in order to increase users outreach, multiple versions of DApps (Decentralized Applications) have to be developed for different public chains, thereby further increasing data fragmentation and users segregation. In order to resolve this pain point, DREP’s proposes the use of Decentralized ID (DID), cross-chain technologies and DREP’s Software Development Kit (SDK) to form the basis of a “connector”, providing easier DApps deployment on multiple public chains with a simplified process while promoting cross-chain data integration and data sharing privacy protection with the use of homomorphic encryption.

As blockchain technology advances from whitepaper research papers towards real world applications and mass adoption, enterprises often lack the technical know-how to fully capitalize on the potential of blockchain technology. During this phase, regardless of whether it is an infrastructure layer or application layer, in order to swiftly penetrate the market and resolve pain points of data fragmentation, a highly productized solution is required. In this aspect, DREP’s unique competitive advantage lies in the ability to develop a flexible and easy-to-use "toolkits" that utilizes a customizable, two-tiered public chain architecture with advanced APIs and Plug-ins support while catering to a number of vertical markets via the DREP SDK.

In summary, DREP’s vision for the blockchain industry is:

- to allow commercialisation of Blockchain with high concurrency.
- to deliver a personalised and seamless user experience for both businesses and consumers along with flexible development.
- to achieve commercialization of Blockchain technology for DApp and enterprise clients, while seeking to eliminate data fragmentation by promoting high levels of connectivity between data silos.

Defining DREP

DREP is committed towards building Connectors and Toolkits based on Blockchain technology, providing solutions that promotes the ease of use, flexibility and frictionless integration. With the technologies behind DREP Chain, ID, Reputation Protocol and SDK, DREP aims to build an open data ecosystem thereby disrupting the current status quo of segregated users and synchronizing fragmented data found on multiple chains.

With the progression of blockchain technology, there has been an endless supply of blockchain projects entering the market. However, they are constrained by their existing infrastructure, and thus only able to serve a small number of applications that are limited in scale and category. On the other hand, large-scale enterprises are reluctant in applying blockchain technology to large-scale commercial scenarios, complicating efforts to increase user adoption in the Blockchain domain.

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

- Poor performance and development experience of public chains.
- Segregated public chain ecosystem and poor user adoption rate.
- A mismatch between Blockchain technology being developed and enterprises' needs.

DREP mainly provides the following technical solutions:

- The DREP Chain is a high-performance public chain that was fully developed in house by the DREP team. It is compatible with EVM and WASM Smart Contracts, and comes with a dual-layer structure constituting of a root chain and customizable 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 data processing with high efficiency, zero gas consumption and strong scalability keeping in mind of security considerations. The use of Smart Contracts will not be able to achieve such outcomes.
- DREP adopts a Schnorr Multi-Signature Algorithm that is based on the Secp256k1 elliptic curve to improve network efficiency and reduce transmission overheads.
- To achieve data connectivity and privacy protection, DREP has designed a Decentralized ID (DID) 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 within one interface.
- To enhance data privacy protection, DREP Chain adopts the use of homomorphic encryption to safeguard users' sensitive information.
- To provide an easy-to-use tool interface for B-end enterprises and provide an efficient and frictionless service portal for DREP Ecosystem users, DREP launched a comprehensive DREP Client integrating functions including asset management, identity management, application development, and traffic portal.
- To enhance the long-term holding value of DREP DID, DREP launched a reputation system. This consists of a general reputation protocol, reputation pipeline interface, reputation data storing and algorithm library, reputation incentive mechanism, reputation account management and fake account identification mechanism, etc.
- To lower the entry barrier and the cost of learning, DREP has developed API, Plug-ins and SDKs for a number of vertical markets. With these toolkits, DApp development teams can deploy on multiple public chains at the same time easily, with built-in wallets and asset trading platforms. With DREP ID, the developers can also acquire users from

various public chain ecosystem, converting them into users and making Super DApps an achievable reality.

- DREP SDK adopts a service-oriented architecture, similar to Java's Spring container development. In most blockchain project code, the modules are more coupled. 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 four different iterations of the DREP Testnets, representing important milestones of the development progress. It also represents the continuous efforts by the team on the product and business development front. With constant communications with enterprise partners, the team is able to act on feedback and explore innovative solutions to eliminate pain points while optimizing user experiences.

DREP's four phases of Testnets are named after Darwin, Riemann, Euler and Planck respectively, paying tribute to the achievements the four scientists had contributed in their respective domains while symbolizing that the team will be on a continuous endeavor to enhance the project’s technology development and commercial application:

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

DREP Proposed Solutions

2.1 Poor Performance and Developer Experience of Public Chains

Performance, usually measured via the Transactions Per Second (TPS) benchmark, is one of the key limitations restricting the adoption of public chains. Payment solutions conglomerate Paypal currently is functioning on around 100TPS whereas Visa, the multinational financial services corporation, is able to handle up to 2000TPS[1]. In contrast, Bitcoin and Ethereum can only process about 10 TPS[2]. The difference in scalability between centralized and decentralized platforms has hindered the growth of blockchain payments applications while also preventing the mass adoption of payment DApps.

With the continuous development of DApps, the volume of data on chain has been increasing rapidly, which resulted in a relentless inflation of resource overheads and has greatly restricted the growth of public chain. Citing an example, EOS RAM's utilization rate is currently around 62%[3] and has impacted the usability of several DApps built on the EOS platform. It is impossible to solve concurrency issues solely relying on protocol layer Smart Contracts to store DApp data[4].

There's also the issue of Scalability Trilemma[5], whereby decentralization, scalability, and security requirements cannot all be satisfied with the existence of opportunity costs. This means that public chains cannot improve on performance without forgoing some aspects of decentralization or security. In view of this situation, DREP has proposed an alternative method to improve scalability via the development of the "Smart Pipeline" technology, which is similar to a Layer 2 solution, to improve batch data processing capabilities.

2.1.1 DREP Smart Pipeline - Improving Data Processing Capabilities

The Smart Pipeline is an innovative blockchain application model proposed by the DREP team. It can achieve high efficiency, zero gas consumption, and robust scalability without impacting security, solving practical needs that could not be solved with the use of Smart Contracts.

While Smart Contracts are widely used on platforms such as Ethereum, issues such as low data capacity, high gas consumption, and lack of active calling functions are often criticized by developers, which negatively restricted 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 via the Smart Pipeline, and the external application executes the result before transmitting the data back to the blockchain client in real-time through the pipeline.

Smart Pipelines can be inserted into every step of the process where necessary to improve the execution efficiency.

[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.

Smart Pipeline Advantages:

- **“Smarter”:** After the Smart Pipeline is deployed on-chain, its execution can be automatically triggered according to pre-specified conditions. In comparison with Smart Contracts, the Smart Pipeline will be able to handle more complex conditions and its execution process will be much more difficult to interfere with, thus being more conducive to the execution of complex transactions.
- **Zero Gas Consumption:** When an application using Smart Pipelines is executed, no gas is required as compared to Smart Contracts. However, zero gas consumption does not mean it encourages non efficient use of resources as all Smart Pipeline codes are required to be open sourced and will be supervised. Moreover, the computing resources that the Smart Pipeline consumes is not part of the corresponding sub-chain, but to be provided by the owner of the Smart Pipeline source code. Thus, even if there is a loophole in the above arrangement, it will not affect the performance of the corresponding sub-chain.
- **No Language Limitations in Programming Coding:** The Smart Pipeline technology uses the WASM virtual machine to execute transactions. Users can write codes in different programming languages and before compiling them into the WASM bytecode. As WASM continues to evolve over time, more languages will be supported, and the code efficiency will also be improved without affecting execution on the blockchain.
- **Meeting the Needs of Complex Applications**: Smart Pipeline applications are not limited by gas and enables blockchain to support more complex applications. Blockchains that adopted the Smart Pipeline technology are still able to interact with other applications or services, meeting the requirements of large and complex applications, thereby allowing for the development of applications which 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 the main chain and sub-chains to improve scalability and the efficiency of the blockchain infrastructure without affecting security or decentralization. In DREP's open-sourced Testnet, **DREP Chain achieved peak TPS of over 12,000** in a public benchmark test conducted on January 8th, 2019.

The test environment conditions were:

- Block time: 10 - 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: explorer.drep.org

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

2.1.3 DREP Consensus Mechanism

PBFT is a safe and efficient consensus mechanism that has been utilised in consortium chains such as Hyperledger[6]. However, existing PBFT consensus mechanisms do not meet the needs of the public chain in terms of consensus efficiency. In the first version of DREP Testnet Darwin, DREP enhances its PBFT consensus mechanism via the use of the Schnorr Multi-Signature Algorithm[7], which allows the integration of a large number of signatures into a singular signatory, thereby improving DREP Chain's efficiencies in terms of storage, network transmission and other aspects, reducing network transmission overheads.

DPOS consensus mechanism selects some node representatives to participate in transaction verification and accounting to get higher performance and faster efficiency. In the following Testnet versions after Testnet 1.0, DREP combines the advantages of two consensus mechanisms, DPOS and PBFT, to achieve better fault tolerance, more stable consensus, more efficient, less prone to fork.

2.1.4 DREP Developer Tool Kits

DREP will provide a series of development resources to encourage DApp and sub-chains development, which includes Docker, IDE and other upper-level tools as well as console and other infrastructure support. Test tools such as browsers, faucets and testnets will also be created to assist developers who are building applications on DREP Chain.

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 Segregated Public Chain Ecosystem and Small Blockchain User Base

The biggest competition in Blockchain industry lies within the “Main Chain” category8, with each main chain striving to become the next flagship product in the blockchain industry, and hence securing the market leader position of being the next ‘Apple’ or ‘Microsoft' in the technology sector. As a result, operability restrictions are common between various public chains varying from the infrastructure layer to DApps which results in segregation of user bases, such as with ETH and EOS users. This inevitably leads to "Prisoner's Dilemma" in the development of public chain.

With DREP ID, DREP aims to assimilate user accounts scattered across various public chains and further expand this model to traditional platforms, allowing more users to access the Blockchain frictionlessly and thus resolving the issue of small user base, promoting adoption and encouraging developers to remove existing barriers between the various public chains.

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.

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

2.2.1 Digital Assets Interoperability

DREP ID supports multi-asset payment and exchange through the DREP Client application, giving users access to a convenient 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 such as asset and data integration, encryption of information, etc. is also available through DREP ID without any interference on the existing numerical systems, loyalty point system, economic system or other aspects of the original platform, thereby forming an interconnected decentralized ecosystem.

This allows DREP ID to support cross-chain 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, the user experience would be improved, user bases would be expanded while reducing unwanted duplications in developments.

2.2.2 DREP ID Integrates Users' Information

One of Blockchain's key challenges affecting user adoption is due to the existence of incomprehensible public key addresses of more than 20 digits. Only a small handful of public chains, such as EOS, have recognized and addressed this issue to a small extent. For example, with reference to EOS, each address registered will require consumption of resources, and thus it will be costly to own multiple addresses.

In order to tackle this limitation, DREP propose to use an alias to generate account names that users can easily understand and remember, which helps to lower the threshold of blockchain usage. Furthermore, managing multiple addresses under one account name results in lower resource consumption, circumvent the requirement of having to memorise public key address of more than 20 digits, but the nickname that users can apply for themselves, stored via 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, while also contributing to a users' credibility and raising awareness to their "second identity" —— the DREP ID.

2.2.3 DREP ID Protects User Privacy

Many centralized platforms analyze and resell users' data without obtaining their consent, in extreme cases, there have been instances whereby users are manipulated into selling their private information. With DREP ID, users have the option to disclose their data. In terms of users' privacy, third parties have to pay to compile such personal information. As a result, users can receive DREP tokens as compensation and third parties can obtain more accurate datasets which includes metrics such as user's reputation value with a lower acquisition cost of obtaining such data, a win-win situation for both.

When logging into centralized platforms, servers have access to sensitive info such as account names, number and email addresses etc. Such platforms are also able to profile users based on their day to day activities without users' notice. DREP ID, combining with third party logging and while avoiding privacy intrusion, gives users the right to choose what information such 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 developed and enterprises' needs

Blockchain is highly anticipated as a tool to innovate production. However, due to its limitations, low efficiency and a lack of development talent to connect blockchain technology with enterprises' needs, the adoption of blockchain technology is moving at a snail's pace.

DREP believes blockchain developers ought not to forecast market needs, but to look deeper within the market and understand the real needs of clients and users. After identifying the pain points and difficulties encountered in blockchain development, one could develop kits for easy integration into a number of vertical markets.

DREP's main solutions fall into two broad categories. The first is to develop DREP technologies into a more mature state to allow APIs and Plug-in support, thus greatly lowering the integration complexity and costs borne by enterprise clients. The second is to develop customized SDKs for vertical domains, solving specific problems in development and forming a complete vertical domain technology solution.

2.3.1 DREP API and Plug-in Support to Promote Integration Ease

DREP's API is adaptable in multiple languages, which provides easier adoption as centralized platforms do not need to invest heavily to perform decentralized modification.

On the other hand, the DREP Plug-in aims to satisfy the more specific and complex needs of vertical markets.

Advantages of DREP API and Plug-in:

1. Allows highly-targeted development without complete comprehension of blockchain technology, making it easier to enrich functionality.
2. Support parallel development and improving the debugging and development processes.
3. Lowers the entry barrier to solving practical problems with Blockchain technology.

2.3.2 Targeting The Vertical Markets via The DREP SDK

The DREP SDK supports a wide variety of DApps. With DREP SDK, DApp development teams are able to deploy on multiple public chains with relative ease, with built-in wallets and asset trading platforms support. Developers can also utilize DREP ID to acquire users across multiple public chain ecosystems, thereby making Super DApps an achievable reality.

Super DApps: DApps that are not confined to a specific public chain, but are connected to various public chains through DREP SDK. Users will be able to pay, transfer, lend and conduct other economic activities without any barrier. At the same time, user education cost are greatly reduced as DREP SDK allows seamless transfer of users from traditional platforms to decentralised version on Blockchain.

DREP SDK for blockchain games has the following features, including but not limited to:

1. Gaming account module: Cross-chain DREP ID removes segregation of user base across different public chains;
2. Payment & trading module: The built-in payment and trading engine can further improve the experience of trading digital asset;
3. Digital operation module: Visualization of operational data and in-game economic system, ensuring transparency and allowing configurability.

DREP Technology Framework

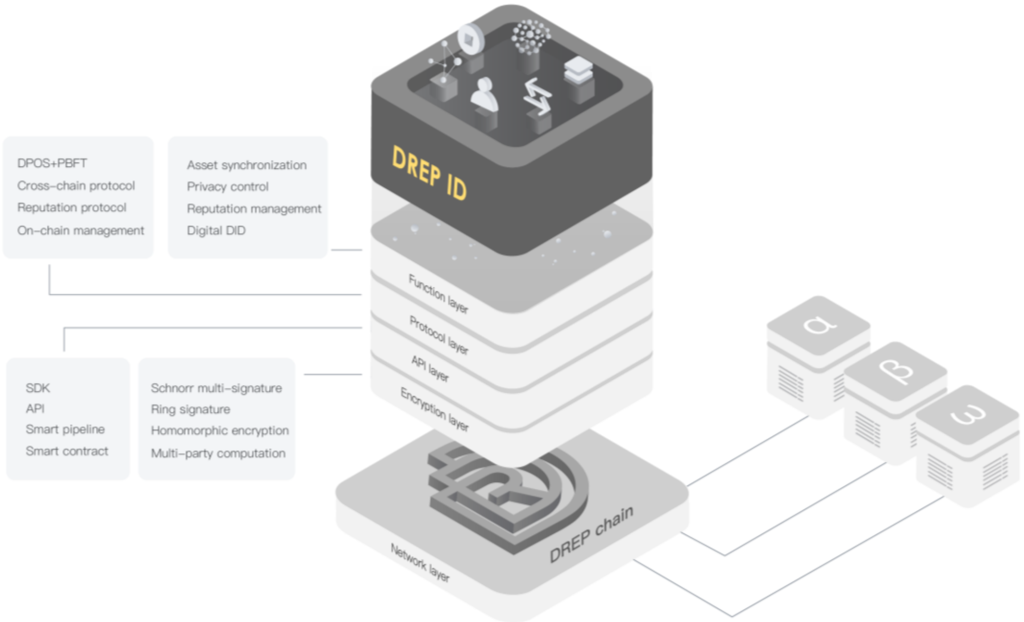
3.1 DREP Public Chain

The DREP Chain is a high-performance public chain that was fully developed in house by the DREP team. It is compatible with both EVM and WASM Smart Contracts and has a dual-layer structure constituting of a root chain and customizable sub-chains. The root chain is primarily responsible for data synchronization to the sub-chains and DREP token transactions, while the sub-chains enables enterprises to develop their own DApps and blockchain ecosystems. This allows enterprises to issue and distribute tokens independently, facilitate deployment of Smart Contracts and Pipelines, while also permitting the exchange of assets and sharing of reputation values across multi-chains.

The DREP Chain prioritizes efficiency when it comes to consensus selection - an improved PBFT was deployed as the consensus mechanism for both the root and sub-chains during the DREP Testnet 1.0 phase. The root chains will also be gradually improved via the adoption of a DPOS mechanism linkage with the reputation protocol.

The technologies behind DREP Chain is based on an improved version of the traditional PBFT consensus mechanism and DPOS consensus mechanism, promoting the adoption of multi-party signature and thus being able to amalgamate the benefits of the DPOS consensus mechanism to improve the efficiency of DREP Chain. The improved efficiency of the DREP Chain is not only reflected in the TPS benchmark, but also in the storage and network transmission process. With the original PBFT protocol, participants are required to transmit signatory details to the leader, before the leader is able to integrate the details onto the block header. With the implementation of multi-party signatories, this process can be greatly improved. DREP Chain utilises the Schnorr Multi-Signature Algorithm, which is based on the Secp256k1 elliptic curve, allowing the singular generation of one signature. As such, this greatly reduces the signature length and thereby reducing the size of the block header, while minimizing the cost of storage as well as the network transmission overheads. Under OPOS mechanism, the evil node can be cleared to make the network more stable and secure.

Illustration of DREP's Technical Structure:



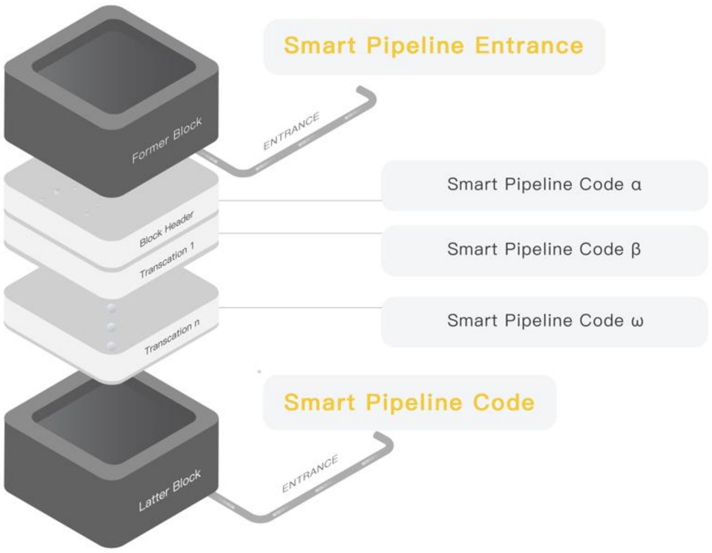
3.1.1 DREP Smart Pipeline

DREP promotes the use of Smart Pipelines to improve bulk data processing capabilities as well as to facilitate the transfers of data between blockchain virtual machines and external applications. As compared to Smart Contracts which are widely used on platforms such as Ethereum, Smart Pipelines offers the benefits of greater efficiency, stronger scalability and zero gas consumption.

Disadvantages of Smart Contracts:

- The maximum data capacity of each block is extremely limited. For instance, with regards to Ethereum's architecture, the maximum usable gas in a single block is 10 million - [9]this means that DApps cannot process large amounts of data or will result in network congestion of the blockchain.
- High gas consumption prevents developers from using mainstream algorithms that are commonly found on traditional platforms, thereby limiting the design of DApps.
- Lack of active calling function, which means Smart Contracts cannot automatically perform complex tasks that will require external script support.

Illustration of DREP's Smart Pipeline:



When a blockchain generates a node, transactions in the node are stored into the virtual machine for execution. Smart Pipelines can be inserted before or after each execution. They function as a program breakpoints and clients can activate them in accordance with their needs. When a breakpoint is triggered, a stop-the-world process would automatically be executed. Real time data will then be transmitted and processed by the external application via the Smart Pipeline. After data processing, the results will be disseminated back to the client on blockchain through the Smart Pipeline. The client will then store the particular dataset onto the database, thereby completing the data linkage to blockchain. Such a process eliminates the drawbacks of huge amounts of data processing in the virtual machine. With the Smart Pipeline greatly optimized by DREP team, the transmission process not only improves operational efficiency and also enhances data processing efficiency.

DREP's Smart Pipeline application consists of the WASM instruction set, which is distributed via blockchain. Applications can also be executed on different sub-chains, and this is also applicable

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

to verified applications that are self developed.

3.1.2 DREP Cross Chain Protocol

DREP's Cross Chain Protocol transcends traditional thinking on cross-chain transactions as it not only provides the basic functionality of transferring assets, but is also capable of synchronizing and migrating behavioral data related to personal identities such as credit rating. Such data are then secured through homomorphic encryption to ensure high levels of security and privacy.

Taking into account of different needs, DREP's Cross Chain Protocol adopts both isomorphic and heterogeneous cross-chain solutions to address performance and cost efficiency requirements found under different architectures:

- **Isomorphic Cross Chain:** DREP main chain and sub-chains are connected via a frictionless isomorphic cross-chain protocol; this allows users to receive real-time updates of their wallets even among different cross-chain platforms.
- **Heterogeneous Cross Chain:** DREP's distributed private key control technology has the ability to connect external chains and traditional platforms to DREP's ecosystem, achieving a more secure heterogeneous cross-chain while extending the application scope of the reputation protocol across multiple platforms.

With the adoption of isomorphic and heterogeneous cross-chain technologies, token assets and reputation data from different DApps can then be integrated with the main account, thereby actualizing a multi-level and dimensional list of user reputational profiles.

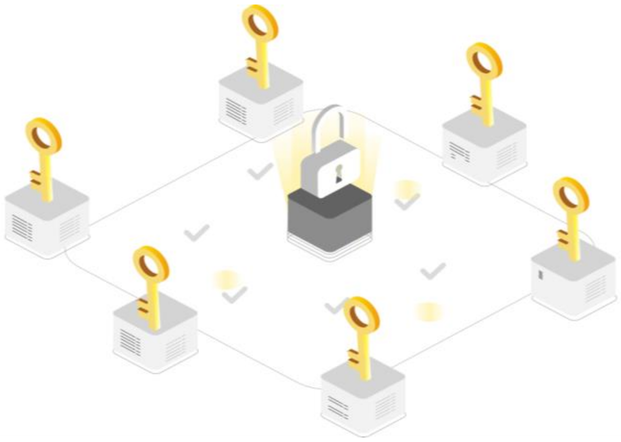
In addition, there are plans to expand collaboration with existing partners on the reputation domain. This will be facilitated by extending the reputation protocol to different systems in accordance with the cross-domain security control requirements, thereby forming an extensive reputation ecosystem while extending DREP's reputation protocol beyond blockchain.

Distributed Private Key Control[10]

DREP's Distributed Private Key Control utilizes decentralized technology to administer cross chain assets with multiple private keys. Account owners retain ownership of the assets, however, with only one singular private key, he/she will not be able to withdraw the assets. They are only able to do so only after obtaining enough private keys via applications with the corresponding chains.

Using an example to illustrate: Alice wants to convert one token via cross chain transaction. A number of nodes on the cross chain, either shards or super representative committees, will maintain one multi sig account on the original chain, while assisting to allocate and administer private keys. It is not possible for a single node to obtain Alice's token from the original chain without possessing enough private keys.

[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.*



When Alice deposits one token to a multisig account controlled by DREP, one equivalent cross-chain token will be generated, which can be traded with other nodes in the ecosystem other cross-chain token with equivalent value. To withdraw the cross-chain token onto the original chain, Alice needs to lock her cross-chain token, which will then release the same amount of tokens on the original chain.

To reiterate, the Distributed Private Key Control technology by DREP provides higher security and privacy while also supports the deployment of Smart Contracts, which includes multi-currency complex contracts. This is regardless of whether the original chain is able to support Smart Contracts or whether it has the ability to perform cross chain transactions.

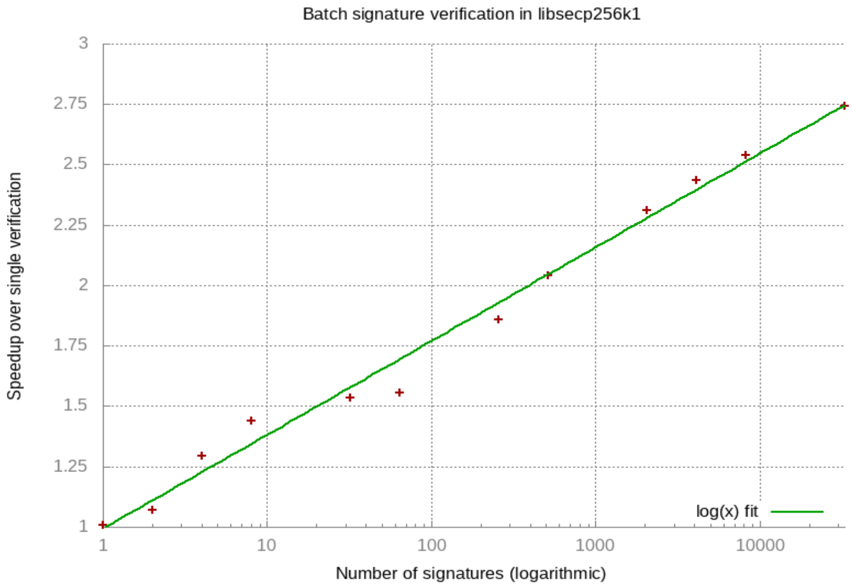
3.1.3 DREP Privacy Protection

Schnorr Multi-Signature Algorithm

A key part of DREP Chain will be the adoption of Schnorr Multi-Signature Algorithm for its PBFT mechanism. The traditional PBFT protocol requires users to transmit signatures to the Leader, whom will then integrate them into the block header. However, with the storage of multiple signatures, this will result in increased sizes of block headers thereby impacting network transmission efficiency. To circumvent such situations, DREP Chain adopts the use of the Schnoor Multi-Signature Algorithm, that is based on the Secp256k1 elliptic curve, thus greatly improving the efficiency of blockchain transmission.

Graphical Exhibit Illustrating the Performance Improvement from the Implementation of the Schnorr Multi-Signature Algorithm[11]

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



In comparison with other signature algorithms, the Schnoor Multi-Signature Algorithm only generates one signature. This greatly reduces signature length and block header size, which in turn lowers the cost of storage and network transmission overhead.

It also provides additional benefits on the privacy front and is known for being conducive towards privacy protection.

Homomorphic Encryption and Privacy Protection

During the deployment of DREP Chain, it is inevitable that information to third parties might be disseminated due to data sharing via the internal Smart Pipeline. In order to eliminate such occurrences and to promote maximum user security and privacy, DREP Chain adopts the use of homomorphic encryption to safeguard users' sensitive information.

DREP Chain's homomorphic encryption utilizes the Paillier technique. It is computed based on the 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[12], 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**

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

A variety of data processing can also be performed after encryption, with the results transmitted back to the users. With the use of private keys, users will be able to obtain the same set of results as with plain text processing, and yet minimizing the possibility of data leakage.

[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.

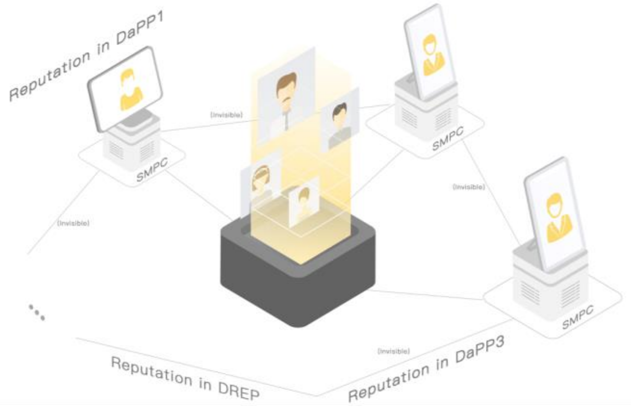
In addition, homomorphic cryptographic signatures could be added to various contents, thereby enabling the possibility to verify misprocessing, spoofing and other forms of misconduct during data processing to ensure data accuracy.

High Security Multi-Party Algorithm[13]

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.

DREP Chain's High Security Multi-Party Algorithm solves the following issue: 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, DREP Chain's High Security Multi-Party Algorithm denies participants the right to access any additional information besides the computation result regardless of whether they have malicious intentions or not.

DREP considers integrating holomorphic encryption, bulletproof[14] to execute Security Multi-Party Algorithm, taking repudiation computation for example.



DREP Chain also deploys the High Security Multi-Party Algorithm to encrypt important data within each DApp and the DREP platform. Users' original data are kept safe even when there is a leakage during the data transmission process. The algorithm ensures parties involved in the data transmission process are able to encrypt and decrypt the data in a much safer manner. Furthermore, users' public key, address and data found on each DApp within the DREP Platform are independent and concealed.

3.1.4 Improvement and Optimization

An integral reason for the development of DREP Chain is to enhance integration with existing enterprise systems. The strong coupling between modules of the main chains of existing

[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.*

blockchains hinders the system integration. Additionally, many high-TPS main chains fail to meet the performance requirements for high concurrent requests transmissions.

Structure Optimization:

DREP modularizes the development of database, network, consensus and other technical features, before storing them separately in containers. A modular call can be performed through middleware, resulting in the decoupling of each module. Furthermore the infrastructure layer is able to automatically implement a series of operations such as the registration, activation and upgrading of the container by way of middleware.

For sub-chain developers, the code of DREP Chain's infrastructure layer boasts clear logic and allows easy reconstruction. In addition, DREP has created a novel routing and message dispatching mechanism which completely decouples the network and consensus layers, increasing the scope of consensus beyond PBFT, thus facilitating independent development of consensus at the sub-chain level.

DPOS+PBFT Consensus Mechanism Optimization

DREP Chain uses DBFT, a new consensus mechanism that is a fusion of the DPOS and PBFT consensus mechanisms. In the DBFT consensus mechanism, the proper operation of the blockchain depends on the trustees, who are fully equivalent. The trustee's responsibilities include:

- providing stable servers to ensure normal operation of the nodes ensuring the nodes will collect network transactions
- ensuring the nodes will collect network transactions
- ensuring the nodes will validate the transaction and pack the transaction into blocks
- ensuring the nodes will broadcast the blocks, and add blocks to their own database after verification by other nodes
- Participating in the governance and maintenance of DREP Chain

The trustee's node will receive block rewards and transaction fee for performing their duties.

Seven trustees will be selected to help operate DREP Chain Test Network 1.0 Darwin. Any DREP token holder can participate in both the trustee election and voting processes. Each token holder's influence on the voting outcome is proportional to their token holdings. Votes can be made and withdrawn any time before the end of the trustee election. Seven users with the highest number of votes at the end of each election will become the trustees of DREP Chain. In return for being responsible for generating blocks and maintaining the system, the seven elected trustees will be rewarded appropriately.

The fundamental purpose of the election is to, based on user voting, select seven highly committed users who may strongly facilitate DREP's development and operations. They are expected to operate nodes to ensure high system efficiency and efficacy and also contribute to the development of the project to the best of their abilities.

- **The specific implementation of the election is shown below:**

```
dlist_i = get N delegates sort by votes
dlist_i = shuffle(dlist_i)
loop
    slot = global_time_offset / block_interval
    pos = slot % N
    if dlist_i[pos] exists in this
```

```
            generateBlock(keypair of dlist_i[pos])
    else
            skip
```

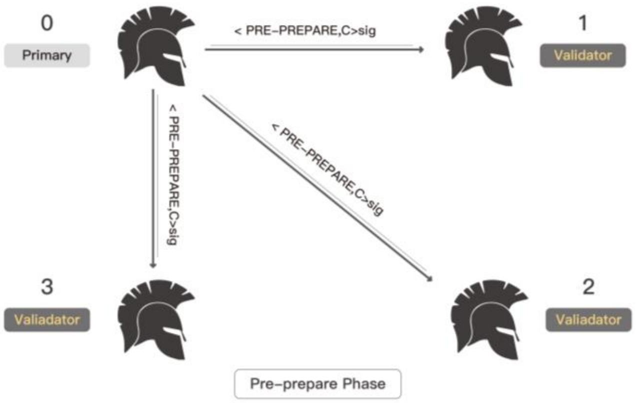
- **Voting Processes:**

  DREP's DBFT is a byzantine-tolerant state machine replication, and is implemented with a three-stage voting process: "Pre-prepare", "Prepare", and “Commit”.

  Phase 1: Pre-prepare

  The Leader is responsible for receiving clients’ requests

  The Leader sends a signed "Pre-prepare" message (view, seq) to other Validators over the network.

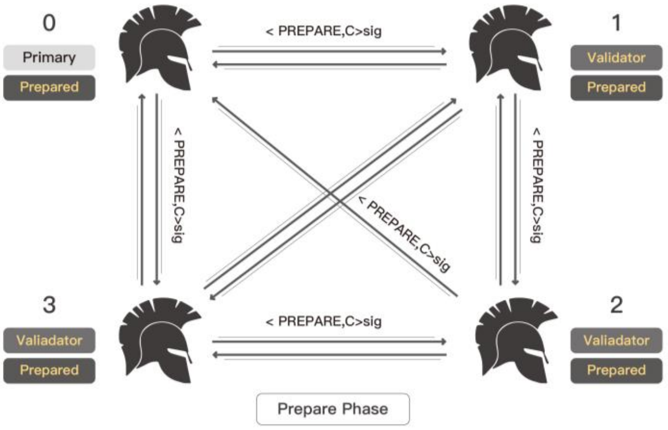


  Phase 2: Prepare

  Each Validator must decide whether to accept the Leader’s proposal after receiving the "Pre-prepare" message. If the Validators accept the proposal, they will send their signed "Prepare" messages to all the other generals, else they will not transmit any message.

  The Validators who sent the "Prepare" message will launch the "Prepare" Phase.

  A general who receives more than three "Prepare" messages will enter into a "Prepared" state. The collection of these "Prepare" messages is collectively referred to as the "Prepared Certificate".



  Phase 3: Commit

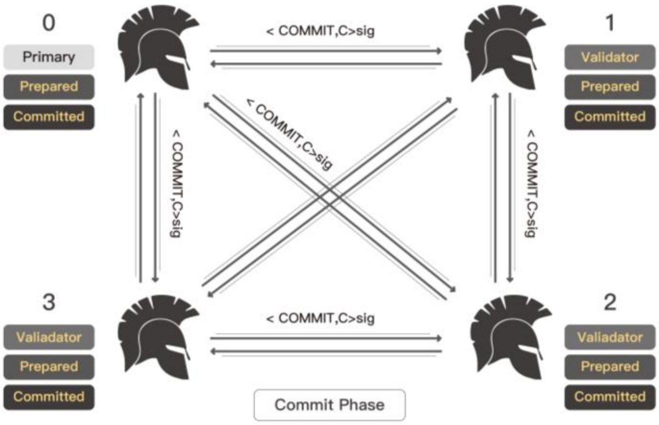
  If a "Prepared" general decides to commit, he will send a signed "Commit" message to all generals, else he will not transmit any message.

The general who sends the "Commit" message will launch the "Commit" Phase.

If the generals receive more than three "Commit" messages, they will perform as instructed by the message. This also means the proposal has reached a consensus.

After executing the instructions of the message, the general enters into the "Committed" state and reports the execution result (Reply) to the byzantine client.

Once the reply has been sent, the current process will end and the general will wait for the next proposal.



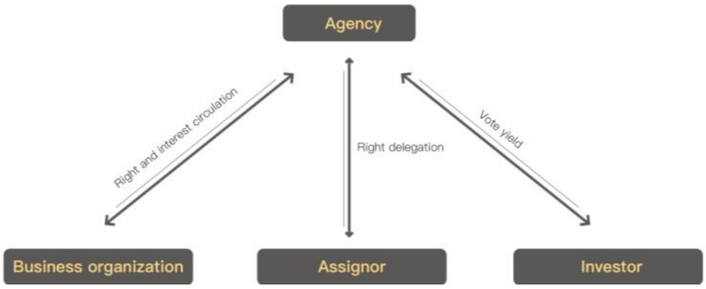
Sub-chain Function Enhancement

A rollback is needed if there is a sub-chain data error during the synchronization of sub-chain data to the main chain., While the original level DB does not support this operation, DREP's self-developed sub-chain nesting and rollback can solve the problems.

DREP Staking Mechanism

DREP token holders interested to participate in the verification of transactions over the DREP network are able to stake their tokens to support nodes in becoming candidate nodes. The staking participant will be rewarded based on the staking duration and amount of tokens staked. When the participant needs the token for other transactions, he can submit a withdrawal request and will receive the staked tokens together with staking rewards in his wallet after the current DBFT cycle.

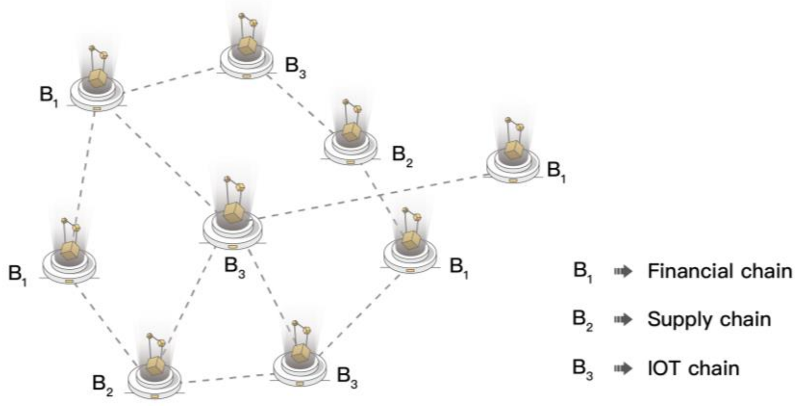
By actively participating in the network system through staking, token holders enhance network security safeguard their rights as token holders and receive staking rewards. Without actively staking, the tokens held do not grant the holder any rights and benefits from staking. Thus, the staking economy is a significant trend for cryptocurrencies and is inseparable from every token holder.



DREP Smart Channel

An independent data cluster called Smart Channel may need to be established between nodes in the DREP network due to data isolation or other special requirements. One of the nodes will broadcast a transaction to create a Smart Channel while the other nodes will apply to join the data cluster created. The influence of each node in this cluster is equal. The nodes can communicate privately, handle transactions independently, and jointly manage all copies of the ledger associated with the cluster. The cluster can be seen to be structured similarly to a circle of friends, although members of the cluster are not necessarily friends. A person may have multiple circles of friends, and each circle of friends has specific activities that they want to do. Different circles of friends can be completely independent or may overlap, but each circle of friends on its own is an entity and has its own "rules".

Co-operation between enterprises or organizations are usually closely linked and may overlap. Suppose that there are four organizations named Org1, Org2, Org3, and Org4, of which Org1, Org2, and Org3 together form a financial chain alliance, while Org2 andOrg4 establish a supply chain alliance. DREP's Smart Channel allows them to build multiple clusters based on specific business needs, creating different consortium chains, and adding new chains in real-time as needed. By supporting clusters, DREP allows a flexible construction of consortium chains under this architecture.



Virtual Machine Optimization:

DREP has improved existing EVM to meet DREP chain's business needs:

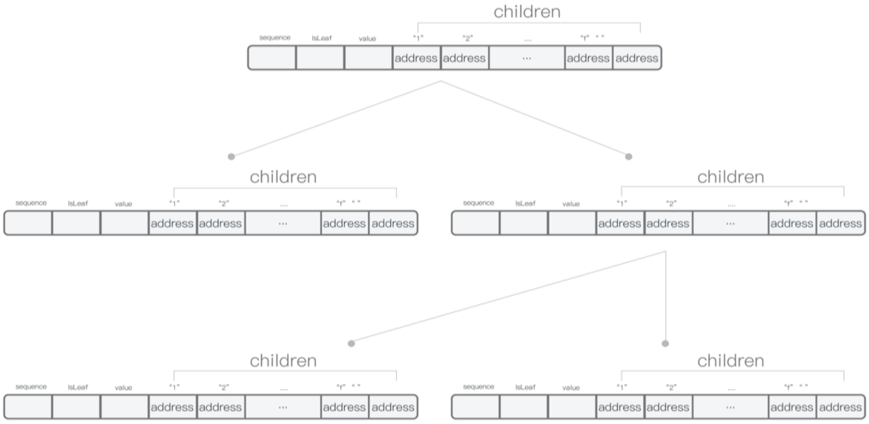
- Added the ability to execute smart contracts on different chains
- Increased reputation-related orders
- Upgraded gas pricing, allowing for automatic adjustments in accordance with configuration and demand on each sub-chain
- Re-designed infrastructure database

Database Optimization

High concurrent requests place great pressure on mechanisms such as caching. This means that blockchains which boasted their 'high TPS' capabilities may not necessarily be able to handle high transaction volumes as marketed. Unlike these blockchains, DREP optimizes the necessary mechanisms such as caches, databases, etc., and uses fine-grained locks inside lRU cache to ensure high performance even when TPS reaches 5,000.

LevelDB database on DREP Chain utilizes Hash Patricia Trie[15] (Hitton Prefix Tree, hereinafter referred to as HPT) technology to store user account status and changes in account status.

HPT is a multi-fork tree data structure. Each node in the tree consists of 4 attributes: Sequence, Value, Children and IsLeaf. The Value attribute of the HPT root node stores the state hash value of the current database for block verification. The Sequence attribute is the only way to get a specific complete Key.



When a user’s account information changes, the database will make corresponding modifications to HPT to reflect the changes in the current database states. Based on the hexadecimal string key of the user account, the database would conduct a thorough search starting from the root node until a certain leaf node has been found. The Sequence attributes of all nodes on the search path are then spliced sequentially to obtain a complete key.

Two Main Advantages of HPT:

- Firstly, the irreversibility and extremely low conflict attributes of the tree structure and hash algorithm improve the convenience and reliability of the database states.
- Secondly, the key value design of the database and data compression capability of the prefix tree greatly improve the efficiency of querying and modifying the database states whilst also reducing computational costs. The database could be updated quickly to reflect the changes to users’ account information by operating the same number of tree nodes as the depth of the HPT. When multiple modifications are made to the account information in one transaction, the increase in computation required to modify the HPT is far lesser than the increase in the amount of account information. The greater the amount of account information, the more considerable the amount of MPT computations could be saved.

Compared with the common prefix tree structure used by Ethereum to save account information, DREP’s HPT unifies and optimizes the design of the tree nodes instead of adopting Ethereum’s method of dividing tree nodes into null nodes, leaf nodes, extension nodes and branch nodes. DREP’s HPT reduces the prefix tree height and thorough search timing, thus improving the query and modification capabilities.

[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.

3.2 DREP Client

DREP Client integrates asset management, identity management, application development, traffic portal, and other value-added services in DREP's ecosystem. Users can store, manage and use a variety of digital assets through DREP Client. An easy-to-use SDK is also provided for developers and enterprises. Users can connect with various public blockchains including DREP Chain through the SDK.

Benefits of DREP Client:

- **Versatile built-in DREP SDK**. DREP Client includes a built-in SDK which allows developers and enterprises from various industry verticals to develop relevant blockchain applications easily.
- **Feature-rich**. Users can enjoy a wide variety of services through DREP Client which facilitates the utility of blockchain applications.
- **Independent and valuable digital identity**. DREP Client not only helps safeguard the ownership and security of user data but also accrue users related benefits.
- **Cross-chain support**. Based on DREP cross-chain protocol, DREP Client supports the storage and cross-chain transactions of multiple digital assets. DREP SDK also allows developers to implement multi-chain interoperability.

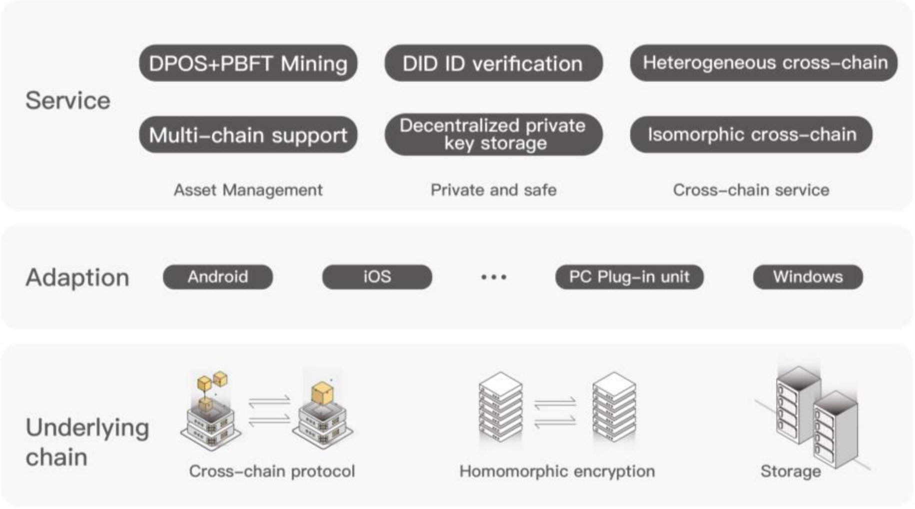
3.2.1 DREP Wallet

DREP Wallet is a highly-secure, multi-chain Hierarchical Deterministic wallet with asset management, privacy features, and other value-added services such as cloud-based custodial service. DREP Wallet version 1.2.0 which was launched in October 2019 currently supports the management of BTC, ETH, BNB, and other mainstream tokens or coins. Being a cross-ecosystem and cross-platform asset management tool, DREP Wallet equips enterprises with the ability to deploy wallet tools quickly.

Key Highlights of DREP Wallet:

- Supports multi-chain, multi-currency asset management
- Facilitates cross-chain interactions
- Provides staking, gamification and other value-added services
- Possesses decentralized private key storage technology
- Is equipped with Digital DID Privacy Protection Technology and Zero Knowledge Proof
- Is further enhanced by homomorphic encryption and other privacy technologies

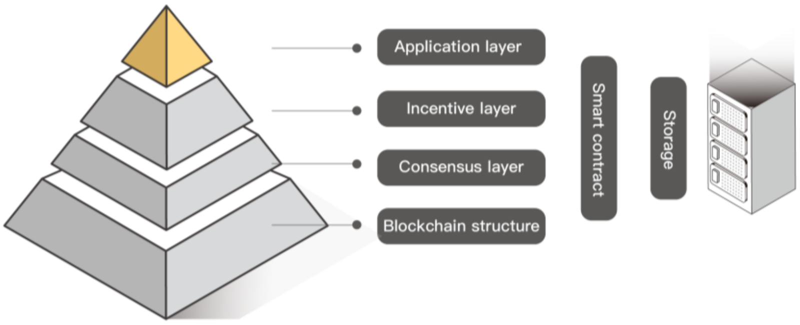
DREP Wallet Architecture:



High Level of Security and Privacy Protection

- **Decentralized Private Key Storage Technology**

  DREP wallet stores users' private keys locally and not on the cloud, which grants a user complete control of his digital assets. Symmetric, irreversible and other encryption algorithms are also used to encrypt user data, allowing the creation of a multi-chain wallet with a single identity as well as the usage of a mnemonic word to manage multiple chains. In order to achieve high levels of security, user data is encrypted and sharded before undergoing data redundancy through storage in nodes located in Singapore, Dubai, India and other countries. Advantages: Safe, reliable, and efficient.

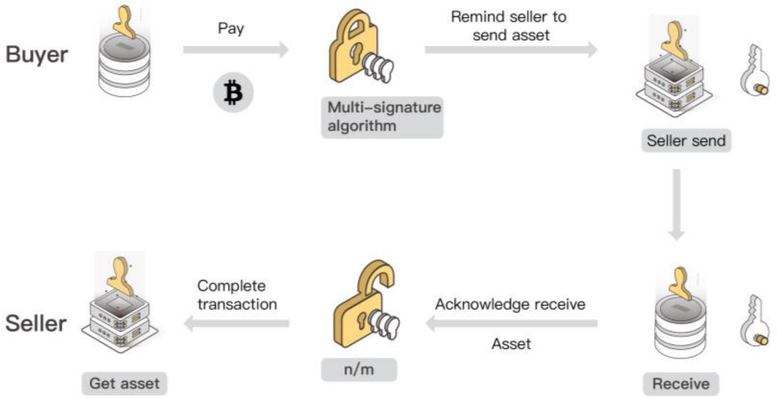


- **Digital DID Privacy Protection Technology and Zero Knowledge Proof**

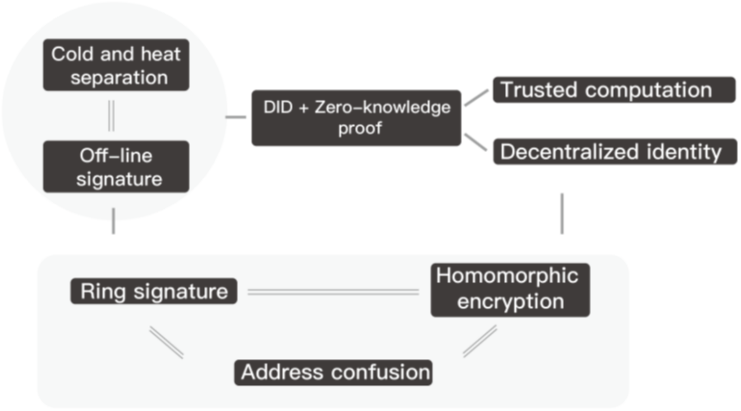
  DREP introduces zero-knowledge proof in DID to prevent leakage of unrelated sensitive information. The corresponding zero-knowledge proof is stored in the DID document as verifiable credentials. With DREP's DID technology and DREP Client, users only need to maintain a single DREP DID private key, to access and manage multiple types of digital assets (e.g. BTC, ETH, etc.).

- **Multi-signature**

  DREP offers m-of-n multi-sig. A public key is obtained from all participating users, where corresponding private key are used to generate a multi-sig transaction, and the public key are announced to other participants. Every participant will use their public key to create a signature with same restrictions (i.e same m, n and list of public keys) to form a multi-sig, creating a multi-sig address beginning with the number '3'. in Pay-to-Script-Hash (P2SH) model, a participant will generate a multi-sig transaction using a multi-sig address. To have the multi-sig transaction broadcast, at least m participants are required to sign off-chain following incomplete signature from previous participants. Multi-sig is especially useful in e-commerce, asset division, co-management of capital and so on.

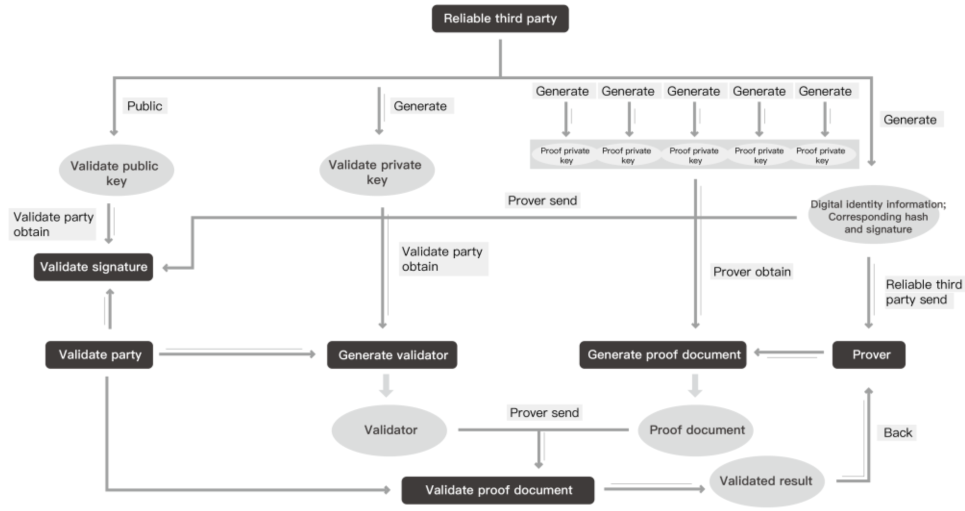


- **DREP Security Technology Library**



DREP introduces zero-knowledge proof in DID

DREP introduces zero-knowledge proof in DID to ensure the security of private data. The corresponding zero-knowledge proof is stored in the DID document as verifiable credential so that private data would not be exposed. With DREP's DID technology and DREP Client, users need only to maintain a single DREP DID private key to access and manage multiple types of digital assets. For example, a verifiable credential D is issued by a trusted third party DID_X to DID_Y. DID_Y's verifiable credential D, which DID_Z wishes to verify, contains information that is irrelevant to the verification needs, while DID_Y wishes to conceal the irrelevant information from DID_Z. DID_Y can negotiate with DID_Z to verify the necessary information of interest via zero-knowledge proof such that his privacy is protected.



Ease of Use and Interoperability

- Convenient usage: With a single key (mnemonics, private key, or Keystore), DREP Wallet supports the management and exchange of digital assets as well as the management of multiple sets of addresses.

- Efficient transaction experience: Provides direct access to block explorer for users to check on-chain transactions easily. Cross-chain transfers will be completed within an hour with real-time progress updates.

- Multilingual support: DREP Wallet 1.2.0 which was launched in October 2019 currently supports Chinese, English, Korean and other languages used in mainstream digital asset market. Support for other languages has been planned and scheduled.

3.2.2 DREP Bridge

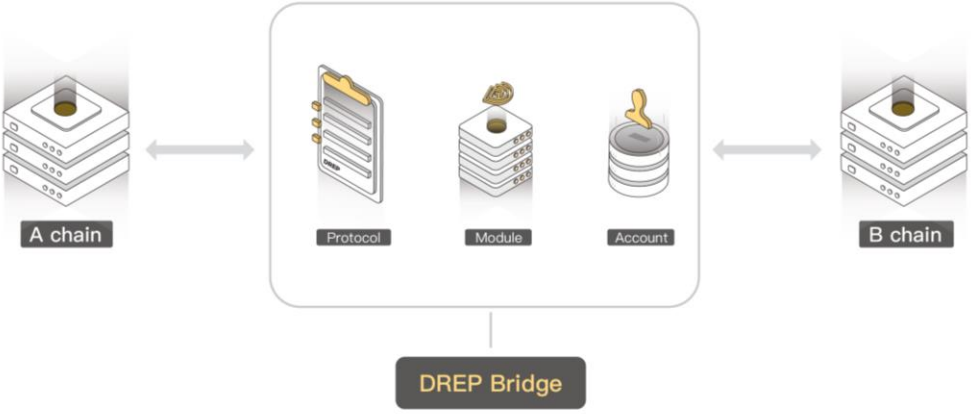
DREP Bridge is a proprietary cross-chain digital asset exchange and trading tool developed by DREP. DREP Bridge allows fast, convenient and secure token swap across different public chains. It can easily be integrated with existing platforms, making cross-chain value transfer a reality, which in turn allows enterprises or users to perform asset exchange, cross-chain transactions and cross-chain asset circulation.

DREP Bridge Benefits:

- Promising business development potential. DREP Bridge supports the convenient and safe exchange of digital assets between any public chains and only needs to be integrated according to enterprise requirements.

- Client with comprehensive features. DREP Bridge Client is currently available in the form of a website, IOS client, Android client. DREP Bridge can be accessed directly through DREP Client or can be built into a partner’s client.

- Fully functional. DREP Bridge allows for efficient use and can effectively reduce R&D costs.



Isomorphic Cross-chain Mechanism

DREP Isomorphic cross-chain is implemented by using smart contracts to achieve bi-directional locking. To perform a cross-chain transfer, the digital asset on the main chain will be locked, while the equivalent assets on the sub-chain will be unlocked. Conversely, when the related assets in the sub-chain are locked, the locked equivalent assets on the main chain will be unlocked.

Heterogeneous Cross-chain Mechanism

DREP Bridge heterogeneous cross-chain is made possible with the additional role, the ‘bridge.’ Based on two-way locking, an extra verification will be done to enable heterogeneous cross-chain operations.

Using the example of transferring 10 tokens from Chain A to Chain B to illustrate the cross-chain interaction:

- Tracking. If a cross-chain transaction is to be performed between Chain A and Chain B, the "bridge" needs to operate light node services on both chains. This allows the block header information to be transferred and received in real-time which facilitates the subsequent implementation of Simplified Payment Verification;

- DREP cross-chain protocol is initialized on Chain A, locking 10 tokens to be transferred cross-chain. The corresponding proof is generated and sent to the "Bridge" through DREP Bridge;

- The "Bridge" receives the proof and verifies that 10 tokens have been locked on Chain A through Chain A's block header, before proceeding to generate 10 equivalent token on Chain B.

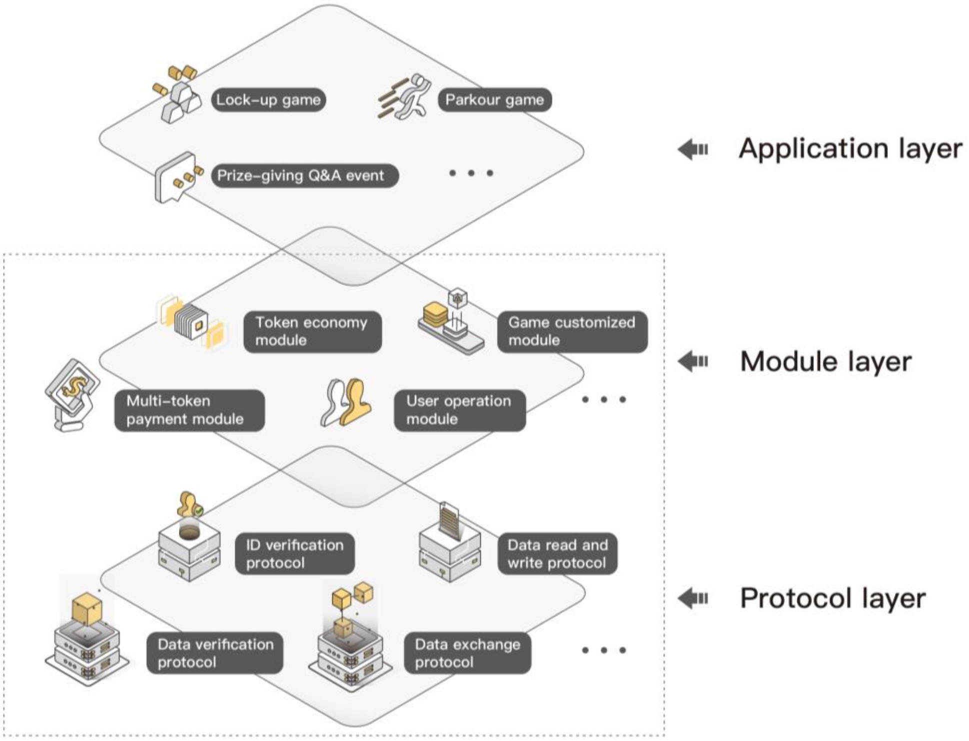
3.2.3 DREP Gamification Tool

DREP Gamification Tool is a toolkit based on DREP SDK. Developers will be able to create economic models, provide asset consumption scenarios, and enable user-defined operations. With the objective of greatly enhancing the token economic system, DREP Gamification Tool is secure, decentralized, has customizable game elements and allows easy integration.

The current blockchain gaming industry faces a multitude of challenges such as lack of games, small user base, high development costs, over-simplistic economic system. In response to these problems, DREP Gamification Tool includes personalized in-game finance module, flexible economic system (including staking mechanism), multi-currency payment SDK, and other features. DREP Gamification Tool is released with the aim of accelerating the adoption of blockchain games and making on-chain economic models a reality.

Benefits of DREP Gamification Tool:

- Customizable gamification module enhances the playability of games and incentivizes users to pay for in-game items.
- Flexible and personalized economic models including staking to meet the needs of different users.
- Supports easy deployment of the game on multiple chains and payment in multiple currencies. This lowers the development costs and increases user outreach.
- Easy to be integrated with and be implemented on Web/iOS/Android clients.



Multi-currency Payment SDK

DREP Gamification Tool supports payment, exchange, storage, and locking of any currency required for public and high-level applications, including transition token and coins issued on different public chain standards. DREP SDK includes a complete payment SDK, developers can implement multi-currency payment function such as clearing and settlement function through simple parameter settings. The advantages of multi-currency payment SDKs and traditional payment channels are:

DREP Gamification Tool supports the payment, exchange, storage, and locking of any currency required by public chains and high-level applications, including transition token and coins issued on different public chain standards. DREP SDK includes a complete payment SDK. Developers can implement multi-currency payment and settlement functions through simple parameter settings. The advantages of multi-currency payment SDKs and traditional payment channels are:

- Low barrier: Payment can be completed with a private key without registration and real name authentication
- Strong liquidity: The blockchain network is global. Digital currency payment is not limited by geography, and users can use digital currency to make payments anytime, anywhere.
- Great convenience: The blockchain network has the "transfer-and-settle" property. Developers can receive the digital currency as soon as the user completes the payment without the need to wait for clearing or settlement.
- Low cost: Peer-to-peer payment without intermediary reduces payment costs.

Digital Asset Consumption Scenario

In order to increase the playability and profitability of blockchain games, DREP Gamification Tool has constructed a wealth of digital asset consumption scenarios which are mainly divided into two modules:

- Game finance module. Developers can independently determine the game's economic model parameters, including the number of tokens to be locked, length of lock-up period, rights to the points earned, additional in-game economic benefits, coupons system, etc.
- Game customization module. This module enables customization according to the personal needs of the users including heroes, props, skins, maps and other in-game elements.

The combination of the two modules greatly enhances the games' playability and incentivizes users to pay for in-game items, providing an efficient and compelling scenario for the consumption of digital assets.

Deflationary Economic Model

DREP Gamification Tool includes a dynamic guidance tool for maintaining an economically-stable token issuance system, which ensures stable or increasing token value. In addition, it also provides data monitoring and visual operation platform. Public chains and application developers can adjust the game economic model in real-time through changing the parameters in the background as well as attract and retain users with in-game financial incentives.

Based on the digital asset consumption scenarios above, as well as DREP Gamification Tool's token economic dynamic guidance tool, public chains and application developers can easily create a decentralized deflationary economic model.

Viral Marketing and User Acquisition Tool

To help public chains and application developers acquire and expand the user base rapidly through viral marketing campaigns, DREP Gamification Tool has built-in tools such as invitation rewards, referral bonuses, leaderboards, etc. Viral user acquisition can be achieved through the game or peripheral products.

Decentralized properties and incentives based on DREP Gamification Tool can assist games to effectively attract users through widespread publicity and communication. The tool's cross-chain capabilities can also help applications reach out to and acquire users of multiple public chains, while the deflationary economy model will help retain users.

3.3 DREP ID

In addition to being the digital identity used on DREP and collaborative application platforms, DREP ID also encompasses user-generated digital images across different platforms. For individual users, DREP ID is the first step to highly secure, private and convenient digital asset management.

For enterprises, DREP ID facilitates the acquisition of user traffic and high-quality data. It also provides a shortcut for cross-chain asset interactions, allowing transactions using a wide variety of cryptocurrencies.

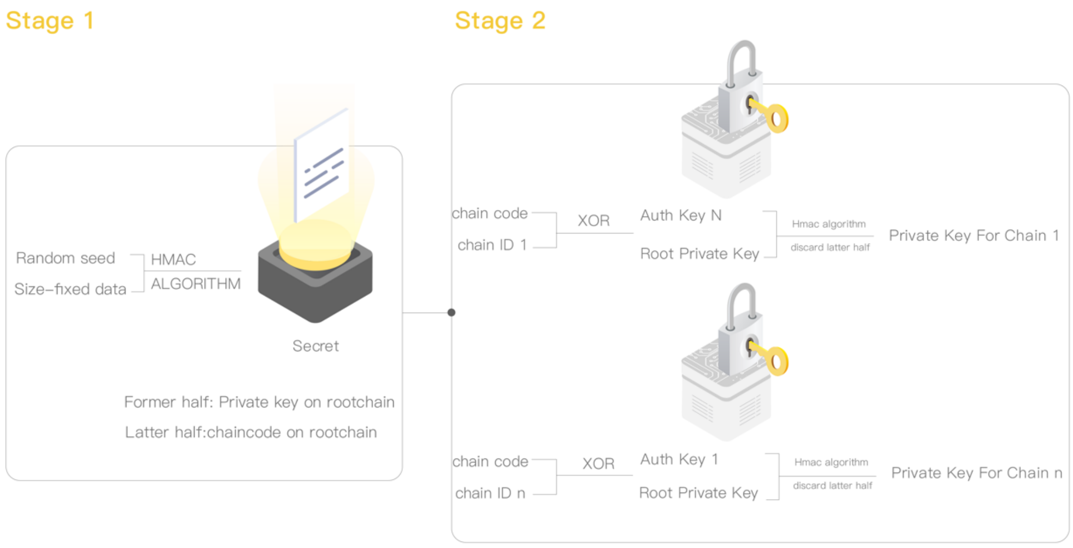
3.3.1 Security

In DREP's 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 Hash Message Authentication Code (HMAC) [16] 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 the master account to control sub-accounts on each application:

- **Master key control**: In order to generate and obtain private keys of sub-chain accounts, users need to utilize the private keys, identity verification codes and sub-chain IDs of the corresponding master account simultaneously. This guarantees the security of the private keys for sub-chain accounts.

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

- **Unconnectable**: Under asymmetric encryption protection, regardless of main or sub-chain, the accounts on each chain cannot be reversely connected, thus ensuring the anonymity of information on-chain.

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

- **Variable address length and higher security**

  DREP uses SHA3's SHAKE256 (SHAKE=SHA+keccak) algorithm[17] to hash public keys, making it possible to vary the output address length, while achieving better performance and greater security.

- **Lower computational costs**

  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', significantly reducing storage and computational costs.

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

3.3.2 Zooko's triangle Breakthrough

The Zooko's triangle is a trilemma of three ideal properties that are generally considered desirable for names of participants in a network protocol.

- Secure: The amount of damage a malicious entity can inflict on the system should be as low as possible.
- Decentralized: Names correctly resolve to their respective entities without the use of a central authority.
- Understandable: Meaningful and memorable (low-entropy) names are provided to the users.

DREP ID's Alias Identity System addresses the limitations of the Zooko's triangle. Users can generate an understandable alias/nickname to represent their ID in a secure and decentralized environment. This ID will be easy to remember and conducive to the users' reputation and profile image.

3.3.3 Universality

Through DREP SDK, DREP ID achieves decentralized login which has the advantages of third-party login and autonomous identity. It also supports the login of a large number of applications and controls the information transferred. Furthermore, DREP ID is compatible with BTC, ETH, EOS and other blockchain architectures, and transcends blockchain limitations such as application location.

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

3.3.4 Convenience

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

3.3.5 Uniqueness

Being decentralized, DREP ID cannot restrict user registration nor force users to perform KYC (Know-Your-Client). Users will ultimately benefit when ID reputation profile image becomes more detailed. As it is more credible to use one unique ID rather than multiple scattered IDs, binding different application accounts to DREP ID in the form of sub-accounts may enhance the users' trustworthiness and reputation.

3.4 DREP Reputation Protocol

DREP Reputation System will complement DREP ID to provide long-term value for ID holders. The reputation protocol enables the design of effective user loyalty systems and facilitates accurate user profiling, greatly improving the quality of B2B2C services.

3.4.1 An Overview of The Reputation System

DREP Reputation System is a comprehensive close-loop ecosystem which includes a general reputation protocol, reputation pipeline interface, reputation on-chain data storage and algorithm library, reputation reward system, reputation value account management and fake account identification mechanisms. In the ecosystem, users' behavior is linked to their reputation which will be evaluated by multiple interacting parties. Users will also receive complete real-time updates on their reputation.

General Reputation Protocol

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

Reputation Pipeline

Reputation Pipeline utilizes Smart Pipeline, which avoids the huge consumption of computational resources by smart contracts and thus improves data processing capability without affecting the performance of blockchain, making real-time user reputation settlement a reality.

Reputation Algorithm Library

DApps cater to a wide range of industries whose needs are very different. The features of DApps catering to the same industry may also vary greatly. Therefore, it is impossible and unscientific to calculate reputation value with a single algorithm. In DREP system, the default reputation algorithm is the summation of the historical cumulative value that decreases continuously over time and the current value.

The reputation algorithm will be provided to DApps to allow customized reputation computation which caters to their business models and needs. DREP System will introduce algorithm templates specifically designed for the following industries, including but not limited to:

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

In addition, DREP will also develop a third-party algorithm library platform with the aim of encouraging developers and DApps to develop their own algorithms and making them open-source. DREP will provide economic incentives for developers contributing their third-party algorithms to the platform.

Reputation Monetization Mechanism

DREP believes that reputation can be monetized. Users with good reputation in the system will be able to receive DREP tokens or rewards provided by third party platforms, effectively monetizing users' reputation data that is stored on-chain.

Reputation Value Account Management and Fake Account Identification Mechanism

Through DREP ID, DREP's reputation system connects every DApp platform and thus connect every user who has reputation value. DREP will strictly manage the reputation value accounts for users in the ecosystem:

- Users can only accumulate reputation values on unique public key addresses and store them on the blockchain within each DApp.
- DREP facilitates every partnering DApp in the accurate categorization, screening and authorization of their users. DREP also supports DApps in providing users with customized services or economic incentives.
- Privacy management: users have the right to manage their reputation value and choose whether to authorize the platform to disclose their reputation value to other DApps and other users.

The DREP team will continuously research and improve fake account identification mechanisms. With the evolution of the Internet, greater popularity of blockchain and increasing assimilation of new technologies such as the Internet of Things with the Internet, fake account identification mechanisms need to be enhanced accordingly.

Through reputation value recognition threshold, Sybil attack prevention mechanism and integration with third-party KYC platforms, DREP aims to minimize the number of fake accounts and encourage users to maintain their reputation and image.

3.4.2 Advantages of DREP Reputation System

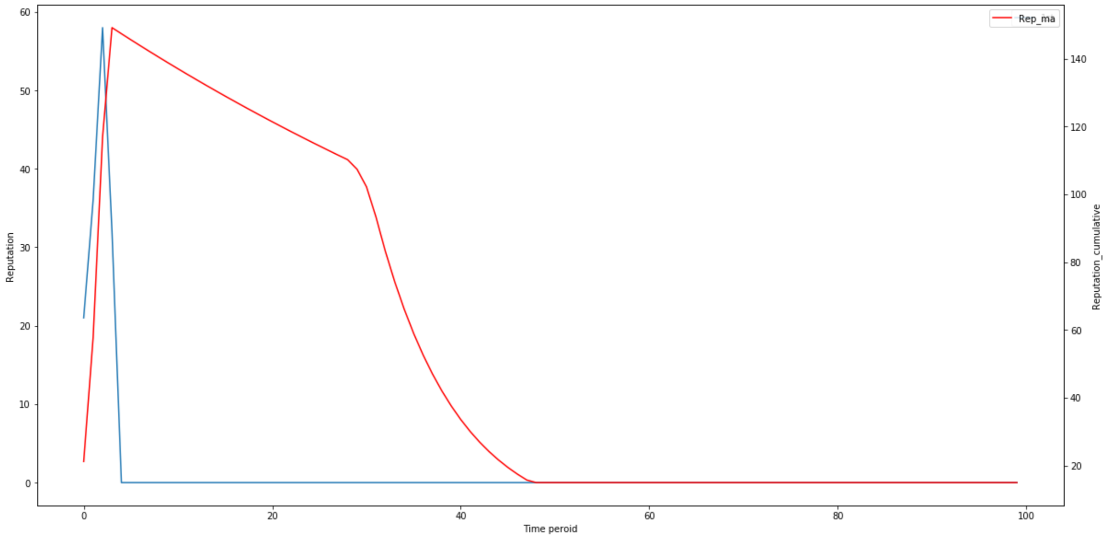
Universality

The Reputation Protocol is not designed for any single platform, but caters to different industries with different templates featuring cross-platform and data integration. User loyalty can be obtained only by adjusting the details according to the industry/platform. Eventually, users may opt to share data within their own scope, thus reducing the cost of data acquisition.

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 daily active usage, and increasing users’ dependence on the platform.

Reputation time-effectiveness, through reputation pipeline, is reflected in the daily or instantaneous user reputation changes. 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 ceases using an application after 3 days, resulting in a reputation loss (The blue line is acquired reputation while the red line is accumulated reputation):



Reputation decays slowly in the early stages and quickly over time, rapidly plunging to a lower value in the later stages. The next time this user activates the same app, the reputation value will commence from the lower value and not start from 0.

Closed-loop Ecosystem

The DREP Reputation Protocol is not only of great importance for enterprise clients but also beneficial for individual users. Through reputation collection, it is able to offer customized preferential treatment, further promoting engagement and consumption, thus forming a closed-loop ecosystem.

3.4.3 Reputation System Complements and Enhances ID

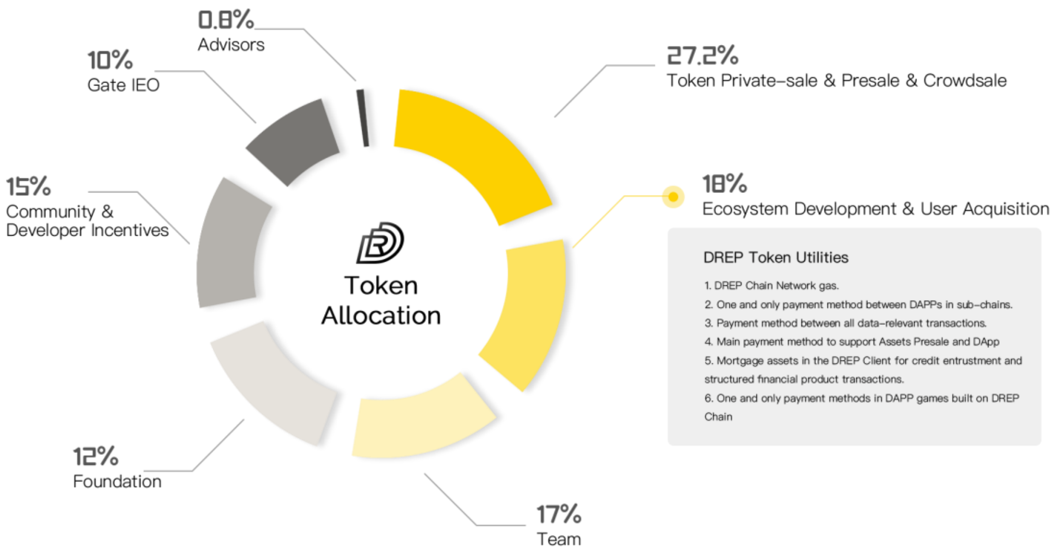
The DREP Reputation Protocol does more than supplement, enrich and replace the traditional points system. The ecosystem of different applications will eventually collectively contribute to the users' reputation image.

Obtaining information from one application is insufficient to portray a user's complete image and interests. To facilitate targeted recommendation and marketing, various data points such as reputation image summarized from multiple applications as well as user's interest and habits extracted through big data analysis could be utilized. This method would be comprehensive and avoids privacy infringement.

DREP Tokenomics

DREP issued a total of 10 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%
  Vesting Schedule:
  Apr. 26th 2019 - 10%
  Jun. 25th 2019 - 15%
  After swap to DREP MainNet Coins - 75%
- IEO: 10%
- Team: 17%
- Foundation: 12%
- Advisors: 0.8%



DREP Token Utilities

1. DREP Chain Network gas.
2. One and only payment method between DAPPs in sub-chains.
3. Payment method between all data-relevant transactions.
4. Main payment method to support Assets Presale and DApp
5. Mortgage assets in the DREP Client for credit entrustment and structured financial product transactions.
6. One and only payment methods in DAPP games built on DREP Chain

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.