DMChain

Decentralized Digital Advertising
Platform on Blockchain

Whitepaper
3.0

Table of Contents

DMChain

Table of Contents

DMChain

Disclaimers

PLEASE READ THIS DISCLAIMER SECTION CAREFULLY. IF YOU ARE IN ANY DOUBT AS TO THE ACTION YOU SHOULD TAKE, YOU SHOULD CONSULT YOUR LEGAL, FINANCIAL, TAX, OR OTHER PROFESSIONAL ADVISOR(S).

This whitepaper is for information purposes only and is subject to change. DMChain cannot guarantee the accuracy of the statements made or conclusions reached in this document.

The information set forth in this whitepaper may not be exhaustive and does not imply any elements of a contractual relationship. The content of this whitepaper is not binding for DMChain (“Company”) and is subject to change in line with the ongoing research and development of DMChain Ecosystem(“Platform”), hereinafter together referred as “Project”.

Nothing in this whitepaper shall be deemed to constitute a prospectus of any sort or a solicitation for investment, nor does it in any way pertain to an offering or a solicitation of an offer to buy any securities in any jurisdiction. This document is not composed in accordance with, and is not subject to, laws or regulations of any jurisdiction which prohibits or in any manner restricts transactions in respect of, or with use of, digital tokens.

ADE Tokens are utility tokens, which are not and will not be intended to constitute securities, digital currency, commodity, or any other kind of financial instrument. ADE tokens cannot be used for any purposes other than as provided in this whitepaper, including but not limited to, any investment, speculative or other financial purposes.

Disclaimers

DMChain is not liable in case of any loss or damage you or anyone else incurs as a result of any activity that you or anyone else engages in based on any information you receive from this whitepaper or as a result of the use of this whitepaper, including, but not limited to the incapacity to use ADE tokens.

ADE tokens are not intended for sale or use in any jurisdiction where the sale or use of digital tokens may be prohibited. ADE tokens confer no other rights in any form, including but not limited to any ownership, distribution (including, but not limited to, profit), redemption, liquidation, property (including all forms of intellectual property), or other financial or legal rights, other than those specifically set forth below.

Certain statements, estimates and financial information contained herein constitute forward–looking statements or information. Such forward–looking statements or information involve known and unknown risks and uncertainties, which may cause actual events or results to differ materially from the estimates or the results implied or expressed in such forward–looking statements. Further, all examples of calculation of income and profits used in this paper were provided only for demonstration purposes or for demonstrating the industry's averages. For avoidance of doubt, nothing contained in this whitepaper is or may be relied upon as a guarantee, promise, representation or undertaking as to the future performance of DMChain and/or ADE token, and/or promise or guarantee of future profit resulting from purchase of ADE token.

Abstract

DMChain

With the disappearance of traffic bonus in the Internet industry, the growth of digital marketing market is slowing down. While being mature, the Internet advertising market growth and market structure are getting more stable. In future, the industry needs to search potential market segment for large-scale commercial monetization. On the one hand, based on the efficiency improvement of the existing stock market, the reform of display advertising in the procedural trading mode is accelerated, and the marketing value is maximized. On the other hand, in the content marketing, information flow advertising and other new marketing methods exploration, the market is driven forward with inventory growth.

As an important trading mode of display advertising, programmatic purchase greatly improves the traffic trading efficiency of all parties in the market.It is recognized by all parties in the market. Various types of suppliers enter the market under such circumstance. However, as John wanamaker, first businessman using modern advertising, said: "Half the money I spend on advertising is wasted; the trouble is I don't know which half." The uncountability of advertising industry and the problem of advertising fraud have a long history and have not been effectively solved. The advent of blockchain technology has the opportunity to effectively solve the "black box" problem that has plagued the advertising industry.

Abstract

DMChain

DMChain, a decentralized digital advertising system, is a subversive transformation of the existing digital advertising industry by using big data and artificial intelligence technology on the basis of blockchain. DMChain has the following characteristics and advantages:

- Real traffic without data frauds
- More efficient and affordable ways to advertise
- Open and transparent programatic advertising, trustworthy and automatic payment
- More accurate and real statistics, direct channel to consumers
- Bring more value to all participtants in advertising industry

In terms of basic construction design, DMChain also uses the third generation blockchain platform Cardano to speed up the rapid landing of products. We have designed four product modules for DMChain ecosystem: DMNetwork, DMExchange, DMID and DMBAAS. We hope to completely transform the advertising industry with blockchain.

- DMNetwork, a blockchain network based on Cardano, enabling Publishers to upload advertising spaces on chain, making each demonstration/click transparent and credible.

Abstract

DMChain

- DMExchange, a decentralized advertising trading platform based on the ouroboros consensus algorithm, based on the data support from DMNetwork, making Advertisers' advertising prices no longer “black box”.

- DMID, the unified account of the advertising audiences in the blockchain world. By Token economic ecosystem, everyone’s data can regain value. On the premise of no violation of user privacy, through the analysis of the data collected in the ecosystem, extraction of audiences’ preference, behavior patterns and group characteristics of Publishers from different categories, interaction with data demander out of ecosystem via DMData API, DMID brings additional economic benefits for the whole ecosystem.

- DMBAAS, a programmatic advertising system based on credible data of the blockchain, providing better delivery tools for advertisers (agencies). It also provides Publishers with more innovation of value monetization based on the blockchain technology.

Project Overview

The Current Market

In 2017, the total revenue of the entire digital advertising industry has hit $563 billion in US dollars. Google and Facebook are the two largest publishers, who jointly own 57.6% of the total revenue, according to a study by AOL and Millennial Media. Big publishers are the dominating power in digital advertising industry.

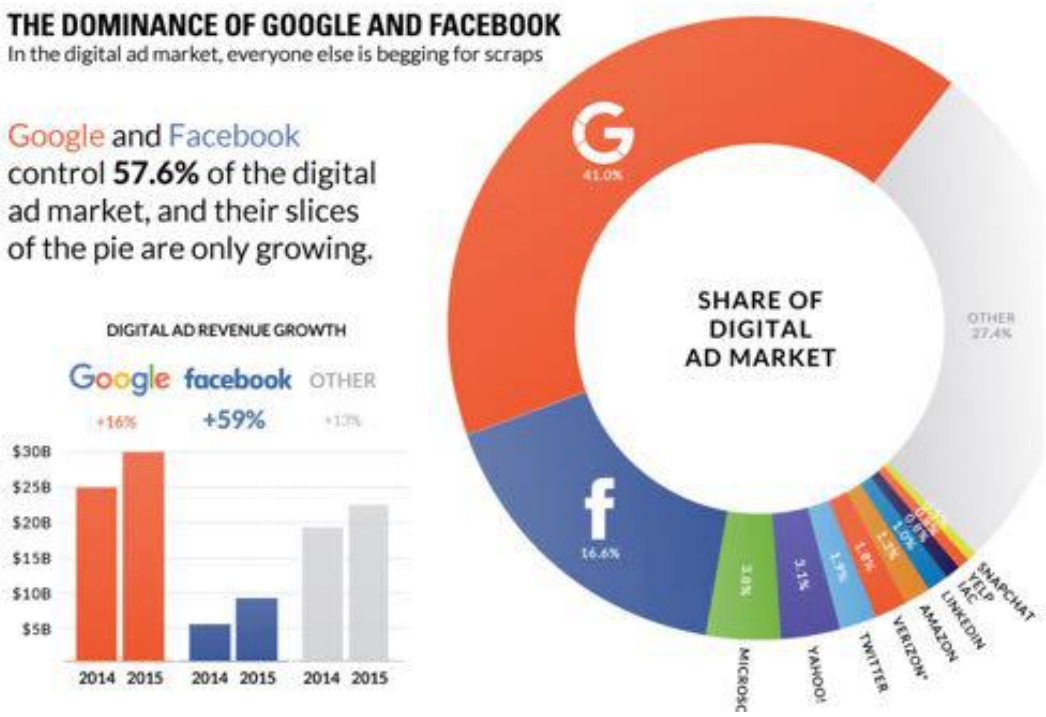

Figure 1. Share of Digital Ad Market

According to the trend, the growth of digital advertising will continue to outperform traditional television advertising. Especially when it comes to programmatic advertising, which is directly related to DMChain's vision, the market share of digital advertising has

increased from 31% in 2013 to 50% in 2018, based on a study conducted jointly by BI Intelligence Estimates, Magna Global, IDC, and the IAB. In the near future, mobile will be the largest digital advertising platform, with video advertising as the fastest growing segment. In fact, YouTube has already become the second–largest search engine in the world, processing three billion searches per month. YouTube today is able to reach more U.S. adults aged 18 to 34 than any cable network. There will certainly be continuous upticks in video advertising through various channels such as smartphones and tablets.

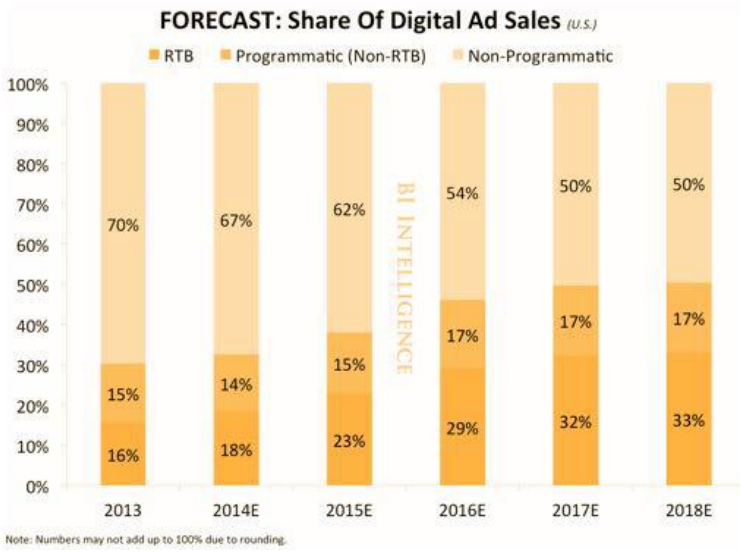

Figure 2. Forecast: Share of Digital Ad Sales (U.S.)

As the number of advertisers and publishers soars continuously, a middleman known as “agency” has also entered into the market to aggregate both supplies and demands. The existence of agencies indeedly made some improvement on efficiencies, however the intermediaries has brought additional costs for the buyers as well. Furthermore, due to the lack of mutual trust among all participants on the value chain, some low–value parties, such as data monitoring, advertisement interception and advertisement verification, have also been introduced.

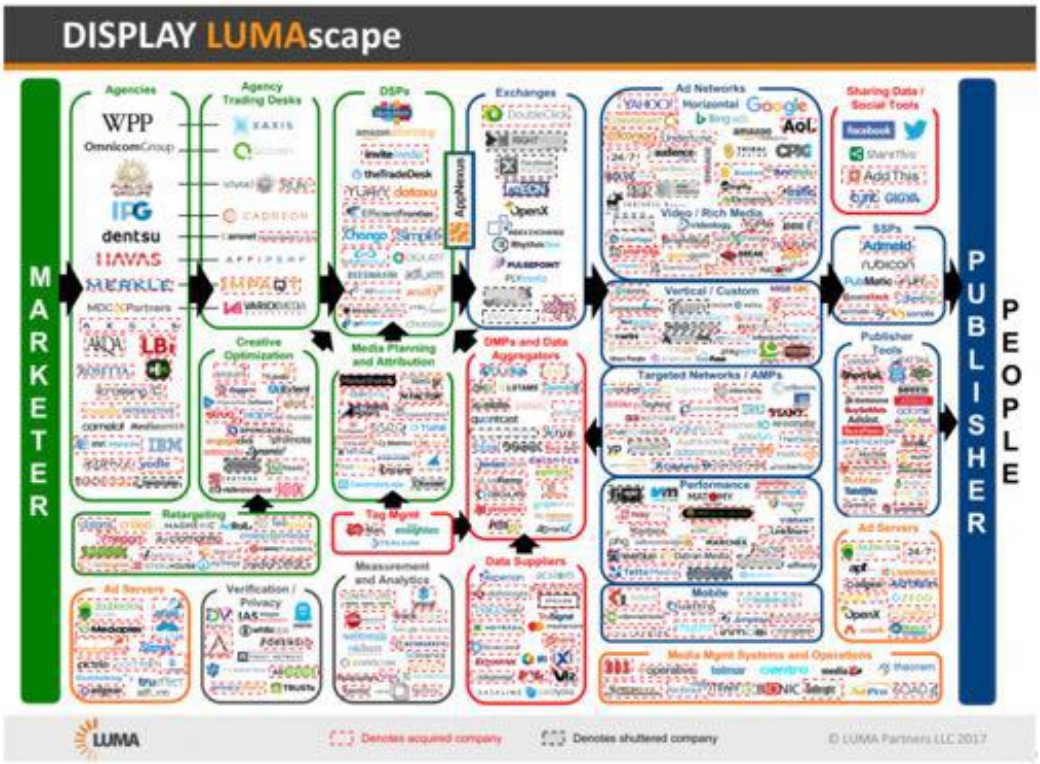

Figure 3. Agencies in Digital Ad Industry

The Challenges

Frauds

Without a trustless platform, the number of advertising frauds is increasing together with the growth of the advertising industry. Advertising frauds, which have been long existed in the industry, do not only ruin the budget of an advertiser, but also raise a trust problem among the industry. According to a study by WPP's GroupM, advertising frauds represent up to 20% of global digital ads spending, which we called "a trust cost". The details were given in the 2017 mobile advertising industry report issued by talkingdata, in where iOS platform has been proven to be the disaster area of advertising frauds. Just in 2017 along, advertisement clicks, a measure used to charge advertisers, has increased 17.8 times.

Project Overview

The problem of advertising frauds has come to a point where it no longer can be ignored. In order to restrain the negative effects caused by frauds, we believe that adopting blockchain technology is a better approach compared to some already existed anti–fraud solution, though the latter may still be evolving. The decentralization and smart–contract features from the blockchain seem to be a natural fit for advertising. With blockchain, advertising ecosystem will definitely be more open and healthier than ever before.

Intermediaries Cost

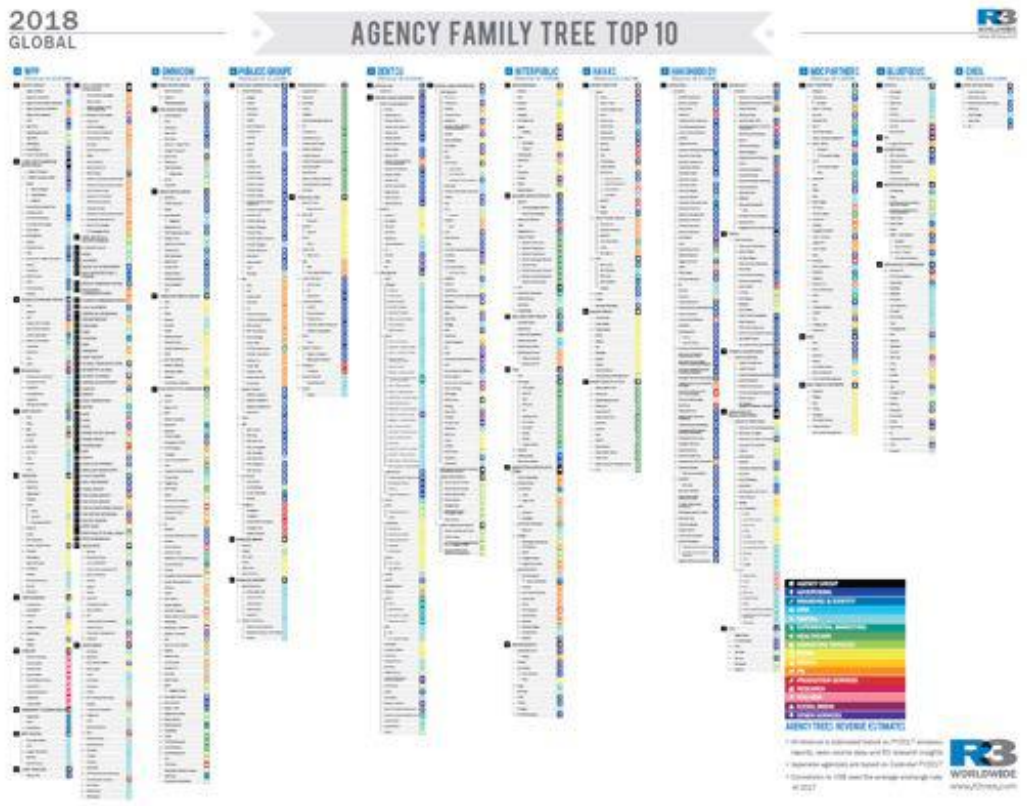

Figure 4. Agency Family Tree

Project Overview

As a highly developed industry, advertising has its own mature supply chain which includes multiple levels of agencies. An agency family, who is responsible for matching the advertiser and the publisher, often takes a big cut from the advertising spending. This adds burdens to both advertisers and publishers, and therefore makes them less motivated. Additionally, in order to reach the most suitable publishers, advertisers usually have to face a long chain of intermediaries, including advertising agencies, media buyers, resellers, affiliate networks, affiliate marketers and advertising networks. Such a long intermediary list results in a very inefficient value exchange.

By building an advertising ecosystem on top of blockchain, the information asymmetry will be eliminated, so the costs of intermediaries will be minimized.

Monetization Difficulty of Long Tail Market

Unlike the top medias and publishers, small publishers generally have very limited room to monetize in traditional advertising ecosystem, simply because the big names in advertising market have taken the most part of the budgets. As a result, small and medium publishers face very narrow choices of boosting revenues. They can't afford neither an expensive agency nor a sales team.

Thanks to blockchain technology, small and medium publishers are now able to monetize in a more diverse environment with the so-called "tokenization economy". DMChain will help small and medium publishers match the most affordable but suitable advertisers, and boost their revenues significantly.

图5. 部分数字广告媒体主

Low Efficiency

While digital advertising market is steadily growing, the anti-ads technology is evolving along with as well. Tools like Adblock has gained enormous popularity, shielding advertisements away from a large chunk of the advertisement viewer base. These anti-ads software has significantly decreased revenues for publishers.

At the same time, there is no a general available manner on collecting results and feedbacks of advertisements. When measuring the efficiency of an advertisement, the advertisers in many cases are forced to rely on data and analysis from either the agencies or third parties. Due to the low transparency of the data, and the fragmented ways of how data is collected, advertisers can hardly know the answer precisely.

Last but not least, both agencies and advertisers are looking for their dream publishers based on their own data. However, it is also challenging to collect data for decision making. None of the players in this industry has the data of the whole viewer base, as they all collect data uncoordinatedly, from their own user base, in their own way. It creates an uncontrollable, chaotic situation: parties usually do not and cannot share their data, and nobody is able to develop a full and precise user portrait.

The Answer: DMChain

DMChain is our answer to address all the challenges mentioned above. Built on top of Cardano, DMChain utilizes smart contracts and data transparency to offer a solution which ensures security, auditability, traceability and ease of use, regardless of the size of an advertiser. Additionally, it removes the distrustness and uncertainties from the advertising industry, and gives advertisers a better picture and control on targeting markets, as well as trackable and quantifiable results.

As blockchain offers access to all its recorded data, combined with deep learning and data mining technologies, DMChain is also able to build more complete and precise user portraits, and anti–fraud mechanisms.

In addition, as we pointed out, the intermediaries costs in advertising industry are significant, and we believe a portion of these costs should be rewarded to the viewers for their attention and time on

advertisements. Moreover, to ensure the consistency of an advertisement in different markets, DMChain also decentralizes the functionality of intermediaries and introduces a new party called “reviewers” in the ecosystem. Reviewers will be rewarded based on their reviewing activities. Apparently, DMChain will bring more value to all participants in advertising industry (except the low value intermediaries).

Figure 6. DMChain connects Publisher, Agency, Advertiser and Audience

Advantages of DMChain

- Real traffic without data frauds
- More efficient and affordable ways to advertise
- Open and transparent programatic advertising, trustworthy and automatic payment
- More accurate and real statistics, direct channel to consumers
- Bring more value to all participtants in advertising industry

The Vision of DMChain

Transparency to end users for advertisers

Advertisers will have access to targeted customers, in which their branding and products are matched through DMChain. Therefore, advertisers can understand their customers better, and then provide suitable products and services.

Monetization for publishers

Product relations of the advertisement industry is changing with the emerging blockchain technology, and traffic magnate won't be able to kidnap the industry any more. The pricing power is returned to publisher itself per real data on blockchain. Tokenization economy provides publishers more channels to monetize.

Project Overview

Monetizing attention of ads audiences

In the era of the internet, personal data is an important source to profit for most of internet companies. However, the value of personal data has never been returned to users. Through blockchain technology, we return the value of user data to the user, and reward advertisement audience for their each attention as they deserve.

Enhancement on agency's procurement

As part of the industry, we believe an agency has its own indispensable value. Due to the highly centralized internet business model, information and value are highly asymmetric. We look forward to breaking up such a black box with blockchain technology. The traffic value shall become more transparent, and the procurement shall become more effective.

How DMChain Works?

DMChain ecosystem introduces ADE Token as the token for value exchange within the ecosystem. The ecosystem consists of four main components: DMNetwork, DMExchange, DMID, DMBAAS, and it Modules.

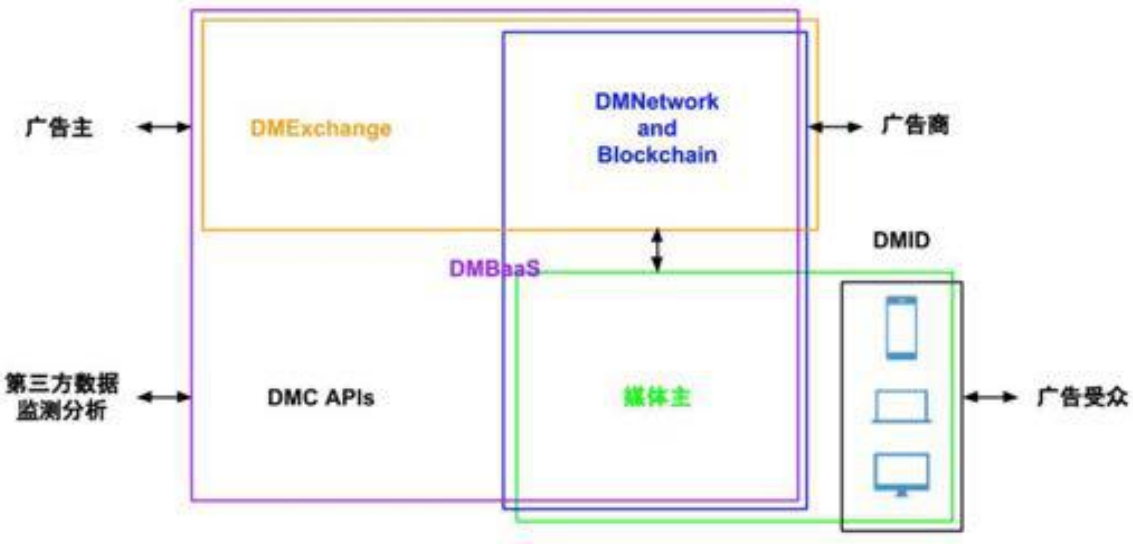

Figure 7. DMChain Components

Modules

DMCoin

ADE Token, the token of DMChain ecosystem, conforms to the ERC-20 token standard and will be freely traded via the Cardano public chain. As the value carrier of DMChain ecosystem, all internal tradings will be based on ADE Tokens. Specific trading and settlement scenarios include but are not limited to:

How DMChain Works?

- The advertiser use ADE Token to pay the Publisher after the display is completed.
- When advertisers participate in the whole process, advertisers use ADE Token to pay Agencies, and Agencies use ADE Token to pay Publishers.
- If the advertiser's display includes watching reward ads, when the audience watches the advertisement or interacts with the advertisement, the advertiser uses ADE Token to reward the audience.
- External data demander uses ADE Token to purchase data from DMChain system.
- After the advertising audience completes the real identity authentication, they are rewarded from the system in the form of ADE Token.

ADE Token

DMNetwork hosts the core logic and smart contracts of the system.It connects advertisers, publishers and agencies, records all kinds of data including transaction records, advertisement audience’ behaviors, publishers’ history reputations, etc,.
Based on ouroboros mechanism, Publishers can upload their advertising resource to DMChain through API. This ensures the transparency and reliability of each advertisement demo because that Publishers’ influence and historical performance can be traced through combined DMID.

How DMChain Works?

DMExchange

DMEchange is the decentralized advertising exchange platform based on the data from DMNetwork. Publishers can publish their advertisement space to the smart contract (traffic resource) on DMChain via the SDK of DMChain system. Advertisers and Agencies will bid for their interested advertisement spaces. Thanks to the ouroboros mechanism implemented by DMExchange, it is built with enough throughput for realizing Real Time Bidding (RTB).

DMID

DMC identification is the unified blockchain based account for advertisement audience to have encrypted accurate user portrait. It allows advertisement audience to manage and unify their on–chain and off–chain personal data. Advertisement audience could choose to authorize DMChain to import their off–chain personal data to enrich their user portrait, which will increase their contribution on ADE Token, as advertiser and publisher will have more accurate match with those additional data. In return, those advertisement audience will receive more tokens as for more complete user portrait. DMID guarantees advertisement audience to be proper rewarded with their attention on advertisement.

Incentive Mechanism

In order to obtain more real and accurate data, DMChain took DMID as the carrier and introduced a set of mechanism to encourage the audience to authenticate the real user information.

How DMChain Works?

In order to verify the authenticity of the audience, the audience needs to conduct KYC real-name authentication. Authentication methods include providing identification documents such as id card and passport at one time, as well as periodically re-authorizing related third-party service accounts. The authentication information is stored in the DMID, which at the same time records the mining power corresponding to the authenticated user information. The mining power obtained by authenticating multiple information can be superimposed, and each authenticated information will increase its mining power. Due to the third party authorization association usually has certain validity, as associated third party user information expire, the corresponding mining power will be deducted. Users can re-authorize the association with third party account information again to restore the corresponding mining force.

ADE Token in TGE and distribution phase will retain a large number of reserved tokens for a contribution reward to participants of the ecosystem. The user providing real certification is one of the main object of contribution reward. These reserved tokens are released slowly and continuously as planned by the predetermined algorithm. When the user stay online through the APP, API, browser plug-in in DMChain, the system will reward currently releasing tokens according to the current online users ability value proportional.

DMBaas

DMBass is the programmatic advertising system on DMChain. It provides better advertising tool for Advertisers, Agency, and more innovative monetization ways for publishers based on blockchain. By implementing SDK or plug-in, DMChain can also exchange data with end users from publishers and data demander can purchase encrypted user data.

How DMChain Works?

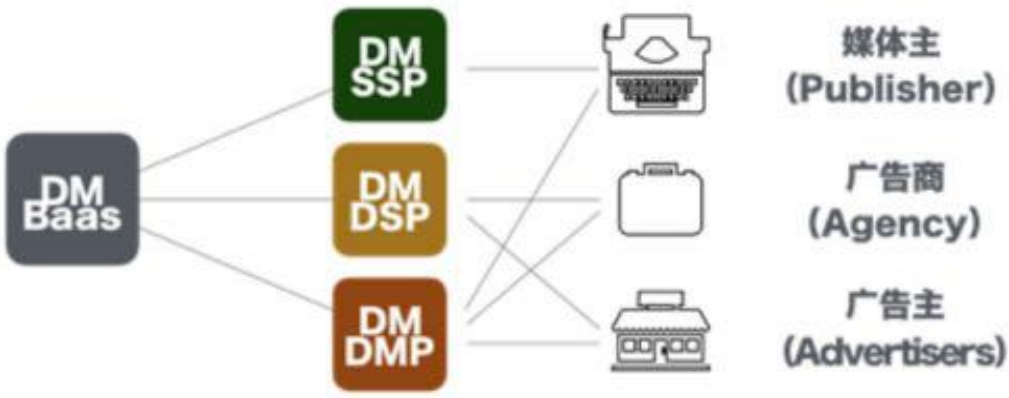

Figure 8. DMBaas

DMSSP provides a blockchain-based supply-side platform for traffic owners and developers who own traffic resources to realize professional, efficient, and rewarding cash flow.

DMDSP offers advertisers an Cardano-based digital advertising smart contract market where advertisers choose contracts according to their requirements. Approved advertisement will be recorded on IPFS and DMChain. Advertiser is able to watch the real-time statistics on Dashboard.

DMDMP supports publisher, advertiser and angency with data mining capabilities based on trustable data in blockchain.

Roles

Advertiser

They are similar to the advertisers in today's digital advertising world. They are the enterprises who want to promote their services or products via advertisements with certain budgets. In DMChain's context, they will have more data and control for targeting market, and they will also have more direct contact with the publishers.

Publisher

They are usually the medias or individuals with large viewer base. In the context of DMChain, publishers can be matched with advertisers much easier, thus they are able to monetize regardless of their size.

Advertisement audience

DMChain advertisement audience are both end users of publishers and DMChain users. They will be rewarded by ADE for their attention to the advertisements. They can also receive rewards by authorizing DMChain to associate their DMID with their user profiles on other external services.

Reviewer

It is a unique functional role in the DMChain advertising ecosystem, a reviewer can be an ordinary viewer at the same time. Reviews will perform decentralized advertisement review, and give collective feedbacks about the advertisement. One obvious benefit is the fraud in traditional centralized advertising systems will be eliminated. Secondly, advertisements can be reviewed in advance by multiple reviewers before its publishment, to conform to local regulation in different regions or countries. If a reviewer makes a correct review judgement, he/she will then be rewarded with ADE for his/her contribution. Viceversa, if a reviewer makes a wrong judgement, a corresponding punishment will then be applied as well.

How DMChain Works?

The following introduces DMChain's algorithm for advertising content review: Content Check Proof of Stake/CPoS

In order to implement the decentralization of advertising content review and avoid the fraud with centralization, before the advertising content is online, it is necessary to get the approval of the content review smart contract. Advertisers need to deposit a certain amount of ADE tokens in smart contracts to initiate the advertising review. To become a reviewer, user must firstly to pledge a certain number of tokens to smart contracts. The higher the number of pledged tokens, the more likely a user is to be chose as reviewer by smart contract. The smart contract will then randomly select 21 reviewers to vote on the advertising content. The selected reviewer needs to give the result within an hour or lose the pledged token. When more than 21 reviewers give the results, the smart contract will automatically reward and punish the reviewers. Rewards and punishments are as follows:

– if more than two–thirds of the reviewers believe that the content has been approved, the advertisement can be released. At the same time, pledged tokens of reviewers who does not approve will be deducted and shared together with deposited tokens to other reviewers.
– if more than two–thirds of the reviewers do not approve the content, the advertisement will not be released. At this same time, pledged tokens of reviewers who approve will be deducted and shared together with deposited tokens to other reviewers.
– otherwise, deposit tokens will be averagely assigned to reviewers whose results are same as the result of most reviewers. And other reviewers won't lose pledged tokens.

DMChain

Data Demander

They are third–parties with demand of user data. They are generally interested in the overall characteristics and patterns of behavior of DMChain users. DMChain can provide highly abstracted statistic in high quality without exposing any individual's privacy. Data demanders will be provided an API to purchase data collected from DMChain with ADEs.

Case Study

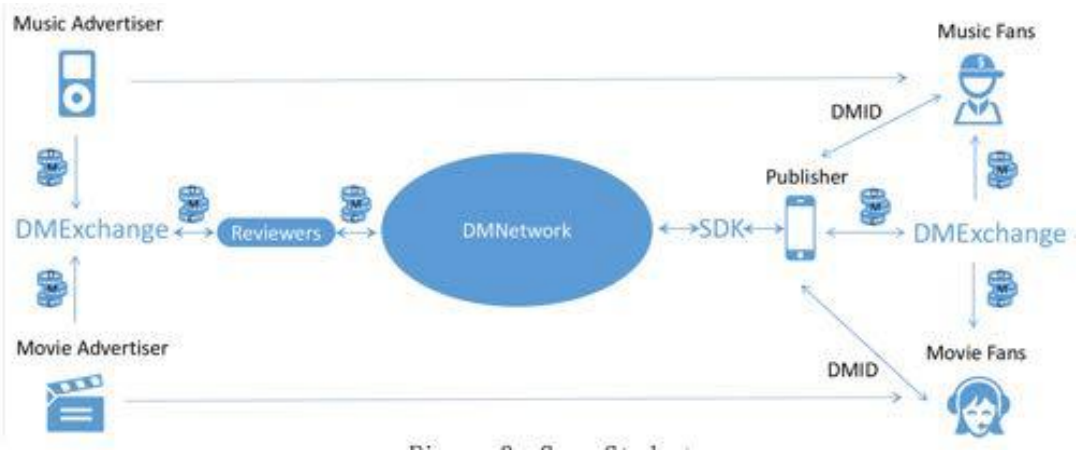

Figure 9. Case Study

P (Publisher) is a social media delicately producing movie and music related contents. Publisher influence two kinds of advertisement audience in the ecosystem, **F(Film Fans)** and **M(Music Fans)**, through its contents like video and article.

How DMChain Works?

The system will provide an API to extract the overall characteristics of P's historical audience from their user profiles. So advertisers like **FA(File Advertiser)** and **MA(Music Advertiser)** can easily know that P's audience will be interested in their products. In addition, the system will also provide an API for the advertisers to query data of P's business profile via his DMID (with P's authorization). So they can access P's historical cooperated advertisers, history of pricing, number of page views, and advertisement interactions. With these supports, FA and MA are able to estimate their cost, and the return of their advertisements on P's channels very well even before the bidding.

When P publish its advertising space to the blockchain based **DMDSP** via the SDK of **DMNetwork**, FA and MA can start their bidding against other advertisers. When they beat other advertisers in the bidding, the result will automatically trigger a state transition in DMChain's smart contract. FA and MA will then receive their advertising space and times on P's channel.

Before FA and MA issue their advertisements, based on the type, content and issued country of the advertisements, the system will randomly select some qualified **R(Reviewer)s** to inspect and audit the advertisement. They will give feedbacks on local legality and effect of the advertisements. After receiving positive feedback of the group review, FA and MA decide to issue and deploy their advertisements. Reviewers who make correct judgement will receive corresponding rewards in tokens and reputation per smart contract terms.

After advertisements are deployed, when **F(Film Fans)** and **M(Music Fans)** start consuming P's contents, the system will analyze each viewer's user profile via his/her **DMID**, select the advertisement with a higher possibility to gain the viewer's attention from FA or MA's advertisements, and show it. In this way, the advertisement could target their audience much more effective, and it also ensures the best return of the advertisers' budget.

How DMChain Works?

DMChain

When audience notice the advertisement and interact with it, some conditions in DMChain's smart contract will be fulfilled and some actions will be triggered. If the advertisement is for **F(Film Fans), DMExchange** will automatically transfer tokens from **FA(Film Advertiser)'s** wallet address to P's wallet address according to previous bidding result. The audience who interact with advertisement will also receive token rewards from **DMExchange** according to the smart contract. All those transaction and interaction are recorded on the blockchain of **DMNetwork**. Both advertisers and publishers can watch statistics of their advertisements in real time.

When **M(Music Fans)** consume P's content, they system will show **MA (Music Advertiser)'s** advertisement, and perform the same process of transaction and recording as discussed above.

Through this case study, we show how **DMChain** successfully resolve the problems such as potential fraud, high agency cost, monetization difficulty of long tail market, low efficiency, bad advertisement effect, and unified data collection trouble.

Community Construction

DMChain community now has mature digital marketing platform DMLei (www.dmlei.com), and first blockchain and cryptocurrency areas artificial intelligence media platform OKZ (www.okz.com), as first batch DMChain community partners.

DMLei (www.dmlei.com) is a digital marketing and promotion service platform for small and medium-sized enterprises. DMLei platform has now aggregated tens of thousands of media and advertising resources to provide one-stop digital marketing services through intelligent SaaS + human services.

How DMChain Works?

DMChain

Based on the resources and operation experience accumulated by DMLei, DMChain is committed to evolve DMLei into the direction of blockchain and create a new community based on DMChain. After tens of thousands of publishers and advertisers successfully migrate from DMLei platform to DMChain ecosystem, they will become earliest participants of DMChain ecosystem which greatly prosper DMChain community.

OKZ（www.okz.com）One of the most comprehensive and influential full-media information service platforms in industry service.

OKZ will be the first blockchain media to access the DMID, providing the unified identification of DMChain account for the advertising audiences. Users accessed with DMID will receive more accurate content push. Meanwhile, users will receive ADE Tokens tokens in return.

DMChain

Technical Solution and Architecture

The DM blockchain ecosystem

The DM blockchain ecosystem for digital advertising is built on the basis of Cardano blockchain and smart contracts with state channels and secure decentralized data storage to create a versatile and robust infrastructure that is reliable under a high ad transaction load. Specifically, DM ecosystem consists of several essential components, including DMNetwork, DMChain, and a large number of middlewares, such as anti–fraud machine learning system, data encryption and etc,. In the following sections, we explain in details the technical designs and implementations of these essential components of DM blockchain ecosystem.

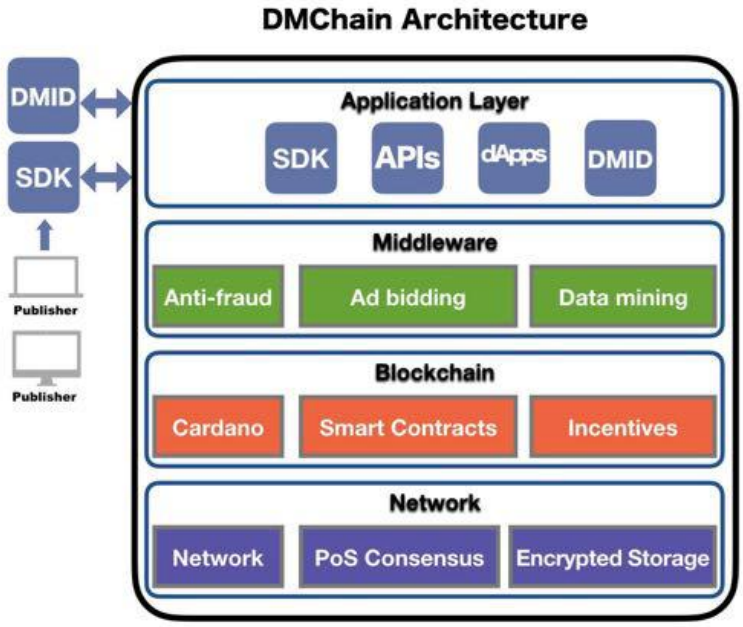

Figure 10. DMChain Overall Architecture

Technical Solution and Architecture

Foundation of DMChain

Blockchain technologies have seen a boom since Satoshi published Bitcoin's whitepaper [1] in 2009. At the moment, there are thousands of various blockchain technologies and architectures in the market, and the quality as well as the technical maturity of such technologies vary greatly, resulting in a rather chaotic situation in the development of blockchain technologies. Overall, blockchain technologies have undergone three different development phases or generations based on their functionality, application scenarios, scalability and performance benchmarks. First of all, Bitcoin as a representative of the first generation blockchain technology takes advantage of Proof–of–Work (PoW) to reach consensus amongst participating nodes. Due to the limitations and characteristics of bitcoin's PoW algorithm, Bitcoin miners have upgraded their mining equipment from CPU to GPU and now to ASIC machines. The costs for mining a block in bitcoin has skyrocketed during the past decade, but the scalability of the bitcoin blockchain has not seen significant improvement, since in Bitcoin, the blocktime is fixed at 10 minutes, which is derived from constants hard–coded into Bitcoin's issuance scheme. As a result of this long block time and PoW mechanism, the bitcoin blockchain today consumes a considerable large amount of energy and resources while supporting a low transaction processing capability (less than 10 transactions per second).

The second generation blockchain technologies represented by Ethereum [2] seek to improve blockchain network's capacity by lowering the block time and introducing a Turing–complete language to support smart contracts. In Ethereum, block time is not a function of the issuance ~~sche~~dule of ether. Instead, it is a variable that is kept as low as possible (which averages about 15 seconds at the moment), for the sake of speedy transaction confirmation. Ethereum has shown that shorter block times are not only technically feasible, but desirable in many ways. While

bitcoin's long confirmation times make retail commerce and other practical applications difficult, when blocks are shorter and transactions move faster, user experience is significantly better. However, since Ethereum inherits PoW mechanism for its consensus algorithm, it has also experienced scalability issues demonstrated by the many network congestions.

To resolve the scalability issue from its roots, the third generation of blockchain technologies represented by Cardano [3] innotivately brings up a Proof–of–Stake mechanism to ensure the scalability, sustainability and interoperability for transactions on blockchains. As blockchain technologies rapidly evolves, new applications on blockchain no longer need to start from scratch with the fundamental blockchain architectures. Rather, they only need to pick a suitable underlying blockchain as their foundation to build new application logic. Since DMChain has high requirements regarding the transaction throughput, reliability and scalability, we opt for the more efficient PoS consensus mechanism. In addition, since Cardano demonstrated its the security and reliability features with rigid mathematical proof, we choose Cardno as our blockchain infrastructure for DMChain.

Cardano

Cardano started its research and development since 2015 and it is now being actively developed by an international team of academics and engineers. Three primary organizations contribute to its development including cryptocurrency research company IOHK led by Ethereum cofounder Charles Hoskinson, the Cardano foundation, and an accelerator called Emurgo. A core component differentiating Cardano from other blockchain projects is "Ouroboros", which is the first Proof of Stake consensus algorithm that is scientifically proven secure. Ouroboros

eliminates the need of high energy–consuming activities in reaching consensus imposed by PoW algorithms. While in PoW systems miners invest their computation power and compete with each other for the right of recording transactions in the blockchain, stakeholders in PoS are randomly elected (in proportion to the amount of stakes they possess) as the slot–leader for bookkeeping transactions. In order to ensure the security of such consensus, the election of slot–leaders has to be truly random. To achieve this goal, Ouroboros innovatively brings up a secure and multi–party coin–flipping protocol to reach consensus. Cardano is built in the Haskell programming language with peer–review and high assurance software standards baked into their development process. Flexibility is a key consideration as development of the platform in planned in layers, to better facilitate ongoing maintenance and easier upgrades over time through soft forks.

Overall, Cardano brings three main advantages to DMChain:

1. Scalability: Cardano enables high throughput with high transactions per second (TPS). Since it is a prerequisite for applications on DMChain to have high transaction throughput, only Cardano can be the suitable candidate. In addition, blockchains are inherently distributed and every participating node in the network keeps a copy of the transaction, these network nodes consumes a large bandwidth to process such incrementals and it leads to scalability issues. Cardano solves this issue using Recursive InterNetwork Architecture (RINA), where each node in RINA belongs to a specific subnetwork and communicates with other nodes when necessary. Also, Cardano processes the ever–increasing amount of transactions through pruning, compression and partitioning technologies.

2. Sustainability: now a lot of companies wish to conduct business related to blockchain technologies and cryptocurrencies, and they would like to raise funding through initial coin offerings (ICOs). However, due to the large number of scandals and over–speculation, ICO activities have not

3. Interoperability: although there are thousands of blockchain and cryptocurrencies in the market right now, it is still not possible to conduct cross-chain transactions due to interoperability issues. The vision of Cardano is to become the Internet of blockchain, where assets can be easily transferred from one blockchain to another. Furthermore, it is possible to bind transaction meta-data with transactions so that a seamless transfer between cryptocurrencies and fiat currencies. In the meantime, thanks to Cardano's support for sidechains, DMChain can achieve independence of code implementation and data under the sidechain architecture, thus reducing the impact of DMChain to the storage of transactions on the main network and achieve a natural data partitioning.

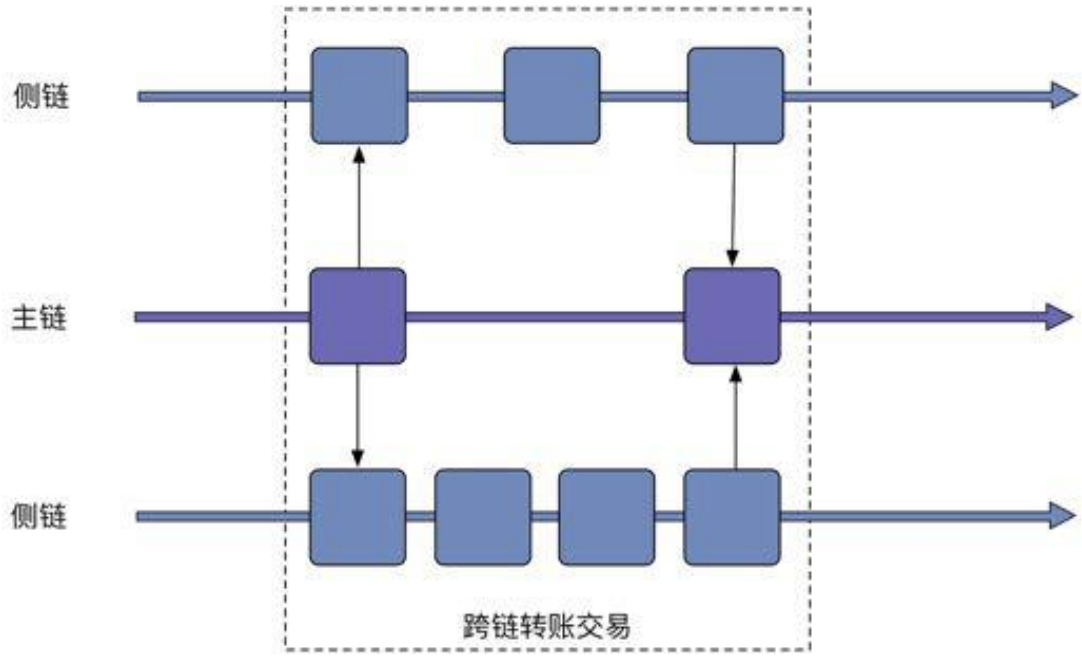

Figure 11. Main chain and side chain interaction

Using sidechain technologies provided by Cardano, one user may move assets from one blockchain to another without predicament. After assets reside on the sidechain, the user can further conduct transactions within this sidechain or eventually transfer these assets back to the main chain, as shown in the figure above.

Based on these advantages, DMChain will built upon Cardano so that it benefits from the state–of–the–art blockchain technology. Furthermore, Cardano's sidechain technology and interoperability would be a great fit to DMChain's application scenario, where interoperations between different chains are both frequent. Finally, choosing Cardano as the foundation of DMChain saves the team a great amount of resources compared to developing a blockchain from scratch.

Smart Contracts

Many application scenarios in digital advertising systems are naturally smart contracts. For instance, after an advertisement is displayed for a number of times and reaches the payment threshold, the advertiser has to pay the publisher a specific amount of money. Such applications can be implemented in the form of smart contracts, so that these business logic can be fully automated. While in legal systems these contracts are bound to specific laws without the need of a full and complete agreement covering all circumstances, in smart contract systems such agreements must be unambiguous since the participating nodes are mainly machines who do not understand the underlying business. As a result, DMChain needs to provide a formalized tool to transform business processes into rigid smart contracts, so that they can operate autonomously on the blockchain.

Current generic smart contract systems usually provides a limited number of instructions or operation codes (opcodes) to support the execution of

smart contracts. In the meanwhile, to facilitate the process of constructing smart contracts, such systems also provide a Turing–complete high–level language and abstraction to help users transforming their business process into opcodes understandable by machines. For instance, Ethereum provides a language named Solidity and Cardano offers Plutus. While Caradno is under active development, it offers a promising platform for operating smart contracts thanks to its high flexibility and scalability. Especially, current smart contracts offered by existing platforms are limited by their low capability and high costs due to data storage for smart contracts. Currently there are techniques for decreasing the amount of data that a single node needs to retain such as pruning, subscriptions (such as partitioning through a distributed file storage system), and some form of compression (including sidechains). Cardano's approach to data storage is to consider each of these solutions and create prescriptive solutions where they may employ these techniques in tandem or in isolation, depending on specific needs, and without compromising security.

To further improve the efficiency of transforming business logic into machine understandable opcodes, DMChain also provides a Domain Specific Language (DSL) [4]. This DSL works on top of Turing–complete languages offered by the underlying blockchain platforms and take the abstraction and encapsulation to a higher level, so that normal users may refer, edit and compile their smart contracts in a visual and user–friendly manner. Besides, users can also simulate the operations of smart contracts without having to deploying them on the main blockchain, so as to save the time and costs for smart contract construction.

DMNetwork

Data Storage and Encryption

Distributed Storage: HDFS

DMChain employs the state of the art distributed storage system for storing its ads and transactional data. We understand the value of clients' data, thus we have stored them in a replicated fashion in the Hadoop Distributed File System [5]. It means that the data is safe even under severe circumstances, such as massive server failures or even data center power outage. We have adopted HDFS after careful consideration. It not only enables DMChain to securely store clients' data, but also allows DMChain to perform big data analytical tasks, such as machine learning and data mining, efficiently. As a consequence, it enables DMChain to leverage the learned insights from data to better serve its clients.

Essentially, HDFS is an Apache Software Foundation project that is a subproject of the Apache Hadoop project. Hadoop is ideal for storing large data (such as terabytes and petabytes) and uses HDFS as its storage system. HDFS allows us to connect nodes (normally virtual machines) contained in multiple computers or clusters, with data files distributed on those computers. We can then access and store data files as a seamless file system. Access to data files is handled in a streaming fashion, which means that applications or commands are executed directly through the MapReduce processing model. Furthermore, HDFS is fault tolerant and provides high throughput access to large data sets. Thus, HDFS is an ideal distributed storage system for our large datasets, i.e., genomic data and medical records.

HDFS has many similarities with other distributed file systems, but there are several differences. One obvious difference is HDFS's "write–once–read–many" model, which reduces concurrency control requirements, simplifies data aggregation, and supports high–throughput access. This is also the major reason why DMChain chooses to use HDFS since ads data are immutable, i.e., they are read only data records and need to be accessed with high concurrency.

DMChain realizes many goals of HDFS. Here are some of the most essential ones:

1. Fault tolerance by detecting faults and applying fast, automatic recovery
2. Simple and reliable aggregation model
3. Processing logic approaches data, not data close to processing logic
4. Portability across heterogeneous hardware and operating systems
5. Reliable storage and processing of large amounts of data scalability
6. Save costs by distributing data and processing across multiple computer clusters
7. Improve efficiency through parallel processing of distributed data and logic to multiple nodes where data resides
8. Reliability is achieved by automatically maintaining multiple copies of data and automatically re–deploying processing logic when a failure occurs

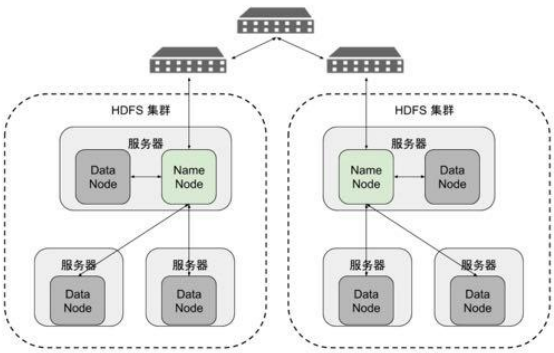

图11. DMChain 多个HDFS集群架构

Figure REF shows the architecture of HDFS deployed at DMChain. Essentially, HDFS consists of a cluster of interconnected nodes where files and directories reside. An HDFS cluster contains a node called a Name Node that manages the file system namespace and client access to files. In addition, Data nodes store data as blocks in files.

In HDFS, a given Name node manages file system namespace operations such as opening, closing, and renaming files and directories. The name node also maps data blocks to Data nodes to handle read and write requests from HDFS clients. The Data node also creates, deletes, and copies blocks of data based on the name node's instructions.

Name nodes and Data nodes are software components designed to run on commodity hardware across multiple heterogeneous operating systems in a decoupled manner. A typical installation cluster has a dedicated machine for running a namenode, possibly a data node as shown in Figure 12. Other machines in the cluster run as data nodes.

Data nodes keep looping and ask for the name node's instructions. Each data node maintains an open server socket so that client and other data nodes can read and write data. The name node knows the host or port of this server and provides information to the relevant client or other data node. Specifically ,all HDFS internal communications are built on top of the TCP/IP protocol. The HDFS client connects to a Transmission Control Protocol (TCP) port open on the Name node and then communicates with the Name node using a Remote Procedure Call (RPC)–based proprietary protocol [6]. The Data node communicates with the Name node using a block–based, proprietary protocol.

DMChain cloud is extremely scalable. We enable the usage of multiple HDFS clusters for storage by interconnecting them with high speed switches as shown in Figure REF. Switches can be directed by any hash

algorithms to locate a specific portion of namespace managed by a specific HDFS cluster.

Hardware Encryption

DMChain envisions a data encryption scenario where data are strictly encrypted even during data processing. It is well known that homomorphic encryption either limits the operations that can be performed on the dataset or leads to significant performance degradation of the system. Thus, we have employed a more advanced encryption technique, i.e., SGX encryption [7]. SGX hardware encryption allows DMChain to protect sensitive client and ad data without sacrificing system functionality and performance. It enables DMChain to build the most advanced and secure storage for client and ad data, which supports any kind of data operations under encryption.

Specifically, SGX stands for Intel Software Guard Extensions. As the name implies, it is an extension of Intel Systems (IA) to enhance software security. This approach does not identify and isolate all malware on the platform. Instead, it encapsulates the security of legitimate software in an enclave and protects it from malicious software. Privileged or non–privileged software cannot access the enclave. That is, once the software and data are in the enclave, even the operating system and the VM hypervisor cannot affect the code and data in the enclave. Enclave's security boundary contains only the CPU and itself. The enclave created by SGX can also be understood as a Trusted Execution Environment (TEE). A CPU in the SGX can run many security enclaves in parallel, which is supported by DMChain middleware.

With the DMChain SGX technology, the system enters a trusted mode for execution by switching the hardware mode of the CPU, using only the necessary hardware to form a completely isolated privileged mode,

loading a tiny microkernel operating system to support task scheduling, and completing the identity certification based on the identity of the authenticated user.

Through the use of DMChain SGX technology, the specific implementation scheme for building Enclave as a fully isolated privileged mode is as follows:

1. Load the virtual machine image onto the disk.
2. Generate secret key certificate for encrypted application code and data. DMChain SGX technology provides a more advanced secret key encryption method. Its secret key is assigned to the user by the SGX version key, CPU key, and DMChain. The new key is generated under the key generation algorithm. This key is used to encrypt the code and data of the application to be loaded.
3. Load the code and data of the application first into the SGX Loader. The SGX loader prepares it for loading into the Enclave.
4. Dynamically build an Enclave in the DMChain SGX trusted mode.
5. The program and data to be loaded are first decrypted by the key certificate in the form of an EPC (Enclave Page Cache).
6. The SGX instruction is used to prove that the decrypted program and data are trusted and loaded into the Enclave, and then each EPC content loaded into the Enclave is copied.
7. Due to the use of hardware isolation, the confidentiality and integrity of Enclave are further guaranteed, ensuring that no conflict between different Enclaves will occur and that they will not allow mutual access.
8. Start the Enclave initialization program, continue loading and verifying the EPC, generate Enclave credentials, encrypt the credentials, and store them as Enclave logos in Enclave's TCS (Thread Control Structure) to restore and verify their identities. .
9. The isolation of the SGX is completed, and the mirroring program in the hardware-isolated Enclave starts execution, and the hardware isolation based on the SGX technology is completed.

DMChain

For accessing SGX Enclave, DMChain SGX authentication algorithm first determines whether the Enclave mode is activated, and then determines whether the access request comes from within the Enclave. If it is positive, then the authentication algorithm continues to judge, if not, it returns an access failure. Based on the credentials before generating the Enclave, they are used to verify whether the access request originates from the same Enclave. If yes, the access is granted. Otherwise, iterate through the Enclave's identity credential record table, replace the next Enclave credential to match until all the Enclaves credentials are tested. If the matching fails, DMChain SGX authentication algorithm returns access failure.

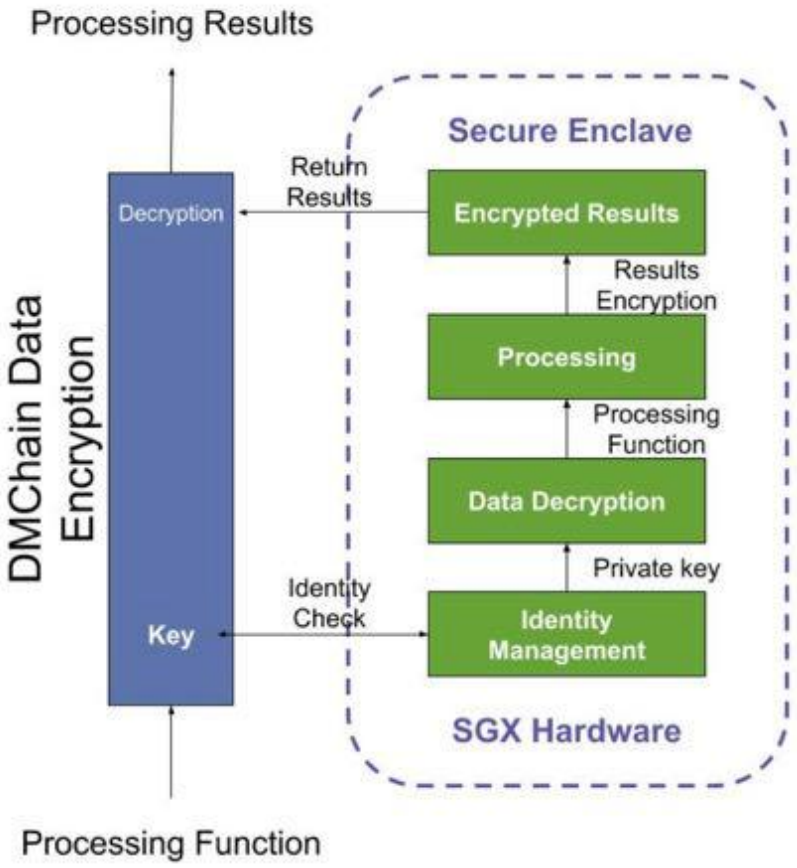

Figure 13. DMChain Processing of encrypted data under SGX

Figure 13 illustrates the processing of a user submitted function in a secure Enclave. First, the user's key is verified by DMChain middleware as well as the Enclave. Then, the enclave decrypts the requested data in the secure Enclave environment. After the data are decrypted, the Enclave processes the data using the user submitted function. Finally, the processing results are encrypted and returned to DMChain middleware, which is returned to the data user after decryption.

Network Layer

As a blockchain grows and more and more users start to take advantage of blockchain for their own business, it is imperative that the blockchain is able to move large amounts of data across a network. As transactions per second increase as the network grows, the blockchain cannot expect to maintain a homogeneous network topology and simultaneously accommodate that growth. This means that each node cannot be expected to relay every message that passes through the network as it grows. To address this challenge, DMChain seeks to implement the Recursive InterNetwork Architecture (RINA) [8] for its underlying network layer。

RINA is an alternative to the current mainstream TCP/IP protocol suite. From its architectural design, RINA allows heterogeneous networking to join the network and significantly increase the data throughput, at the same time ensuring the security and privacy of data transmission. The main difference between RINA and TCP/IP is that all networking nodes in RINA are participants of Inter–Process Communication (IPC) [9]. Since the IPC in different network layers is limited to specific domains and scale, RINA in essence is a set of recursive protocols instead of a set of ad hoc communication protocol implementations。

Technical Solution and Architecture

The architecture of RINA is shown in the figure below, where a Distributed Application Process (DAP) is a computer program for a specific purpose in the information processing system. It consists of one or more application entities and computation resources associated to the DAP, such as processors, storage and IPC. IPC Processes (IPCP) are a core part of RINA, and they also constitute as a part of the Distributed IPC Device (DIF), which is responsible for local implementation and supporting the management of IPCPs.

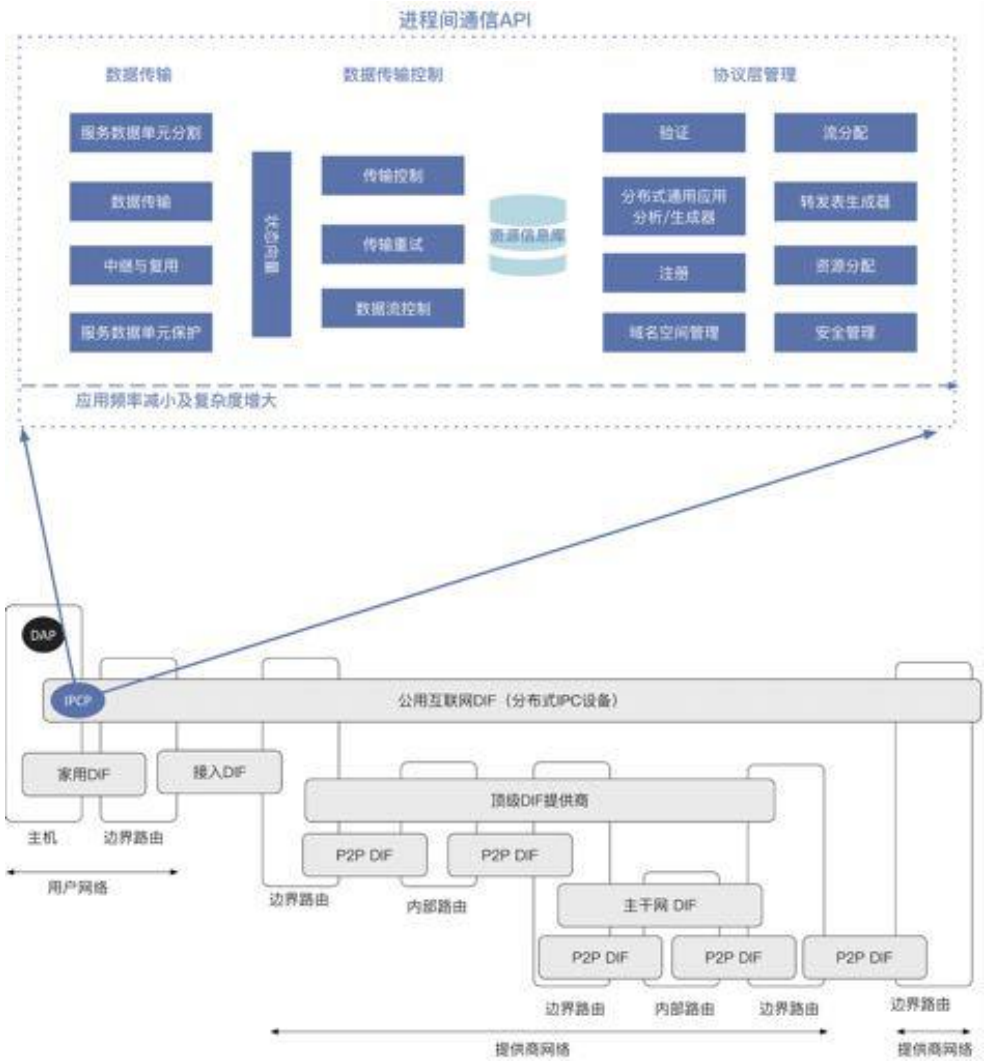

Figure 14. Network Layer

DIF in RINA is a collection of DAPs and is responsible for task scheduling and cooperation of IPC tasks. DIF provides IPC services a set of APIs to participate in the process of exchanging information with another application in the same domain. And DIF can be divided into different categories based on its application domain as well as its processing capability, including home DIF, access DIF, P2P DIF, backbone DIF and public internet DIF. These DIFs help realize high performance, high reliability and high security in the data transmission process and support fast data synchronization and read/write operations.

Provably Secure PoS Consensus Algorithm

Provably Secure PoS Consensus Algorithm
Using PoS for a cryptocurrency is a hotly debated design choice, however because it adds a mechanism to introduce secure voting, has more capacity to scale, and permits more exotic incentive schemes, PoS is becoming increasingly popular. The PoS consensus algorithm used by DMChain inherits from Cardano and it is named Ouroboros, which provides a provably secure PoS consensus mechanism. The core innovation it brings beyond being proven secure using a rigorous cryptographic model is a modular and flexible design that allows for the composition of many protocols to enhance functionality. This consensus mechanism will keep costs low, because it's a system that allows for parallel growth, and also because it potentially allows for maintaining multiple chains concurrently. Ouroboros has a high assurance that the conceptual design of their system is correct since it has undergone a long peer review process.

PoS algorithms ensures a much higher transaction throughput and at the same time guarantees the security of voting processes. Ouroboros is modeled using psi calculus [10], which is a formal modeling language that is machine understandable, making it highly secure. Specifically, it can effectively prevent a wide range of attacks, including:

1. Double spending attacks: In a double spending attack, the attacker tries to transfer an asset multiple times and to revert a transaction that is confirmed by the network. The objective of the attack is to issue a transaction, e.g., a payment from an adversarial account holder to a victim recipient, have the transaction confirmed and then revert the transaction by, e.g., including in the ledger a second conflicting transaction. This type of attacks is not feasible in Ouroboros since the attacker has to bring the system to a state where the confirmed transaction is invalidated.

2. Transaction denial attacks: In this type of attacks, the adversary wishes to prevent a certain transaction from becoming confirmed. For instance, the adversary may want to target a specific account and prevent the account holder from issuing an outgoing transaction. Such an attack is not feasible since the liveness of the network ensures that as long as the transaction is attempted to be inserted for a sufficient number of slots by the network, it will be eventually confirmed.

3. Desynchronization attacks: In a desynchronization attack, a shareholder behaves honestly but is nevertheless incapable of synchronizing correctly with the rest of the network. This leads to ill–timed issuing of blocks and being offline during periods when the shareholder is supposed to participate. Moreover, a desynchronization may also occur due to exceedingly long delays in message delivery. As long as 50% of the participating nodes in the network are synchronized, such type of attacks will be impossible.

4. 51% attacks: A 51% attack occurs whenever the adversary controls more than the majority of the stake in the system. It is easy to see that any sequence of slots in such a case is with very high probability forkable and thus once the system finds itself in such setting the honest stakeholders may be placed in different forks for long periods of time.

Such attacks is not possible in Ouroboros since the initial stake allocation is a very careful and controlled process so that it become impossible for a specific party to gain more than 50% of the total shares.

5. Selfish–mining attacks: In this type of attack, an attacker withholds blocks and releases them strategically attempting to drop honestly generated blocks from the main chain. In this way the attacker reduces chain growth and increases the relative ratio of adversarially generated blocks. In conventional reward schemes, as that of bitcoin, this has serious implications as it enables the attacker to obtain a higher rate of rewards compared to the rewards it would be receiving in case it was following the honest strategy. Such attacks is not possible in Ouroboros since selfish mining attacks are neutralized and the attackers will not receive any benefits from such behaviors.

It is obvious that this is an incomplete list of attacks Ouroboros is immuned from. Thanks to its provably secure nature, we choose it as the consensus algorithm for DMChain. This algorithms allows us to minimize the operational costs and at the same time suport parallelization of growths and sidechains. As a result, DMChain will be of high security, high reliability and high scalability.

Ouroboros Consensus Algorithm

We first provide a general overview of Ouroboros protocol design [3]. The protocol's specifics depend on a number of parameters as follows: (i) k is the number of blocks a certain message should have "on top of it" in order to become part of the immutable history of the ledger, (ii) ε is the advantage in terms of stake of the honest stakeholders against the

adversarial ones; (iii) D is the corruption delay that is imposed on the adversary, i.e., an honest stakeholder will be corrupted after D slots when a corrupt message is delivered by the adversary during an execution; (iv) L is the lifetime of the system, measured in slots; (v) R is the length of an epoch, measured in slots. We present our protocol description in four stages successively improving the adversarial model it can withstand. In all stages an "ideal functionality" $F_{LS}^{D,F}$ is available to the participants. The functionality captures the resources that are available to the parties as preconditions for the secure operation of the protocol (e.g., the genesis block will be specified by $F_{LS}^{D,F}$).

$$F_{LS}^{D,F} = f(D, F, L, S)$$

Stage 1: Static stake; $D = L$. In the first stage, the trust assumption is static and remains with the initial set of stakeholders. There is an initial stake distribution which is hardcoded into the genesis block that includes the public–keys of the stakeholders, $\{(vk_i, s_i)\}_{i=1}^{n}$. Based on our restrictions to the environment, honest majority with advantage is assumed among those initial stakeholders. Specifically, the environment initially will allow the corruption of a number of stakeholders whose relative stake represents $\frac{1-\varepsilon}{2}$ for some $\varepsilon > 0$. The environment allows party corruption by providing tokens of the form $(Corrupt, U)$ to the adversary; note that due to the corruption delay imposed in this first stage any further corruptions will be against parties that have no stake initially and hence the corruption model is akin to "static corruption." $F_{LS}^{D,F}$ will subsequently sample which will seed a "weighted by stake" stakeholder sampling and in this way lead to the election of a subset m of keys $vk_{i1}, \ldots, vk_{im}$ to form the committee that will possess honest majority with overwhelming probability in m , (this uses the fact that the relative stake possessed by malicious parties is $\frac{1-\varepsilon}{2}$; a linear dependency of m to ε^{-2} will

be imposed at this stage). In more detail, the committee will be selected implicitly by appointing a stakeholder with probability proportional to its stake to each one of the L slots. Subsequently, stakeholders will issue blocks following the schedule that is determined by the slot assignment. The longest chain rule will be applied and it will be possible for the adversary to fork the blockchain views of the honest parties. Nevertheless, we will prove with a Markov chain argument that the probability that a fork can be maintained over a sequence of n slots drops exponentially with at least $\sqrt{n}$, cf.

Lemma 1. correct party consists the majority in the algorithm by satisfying the following formula:

$$N_{malicious} = \frac{1-\varepsilon}{2} * N \preccurlyeq \frac{1}{2} * N, where\ \varepsilon \succ 0$$

Stage 2: Dynamic state with a beacon, epoch period of R slots, $R = \ominus(K)$. The central idea for the extension of the lifetime of the above protocol is to consider the sequential composition of several invocations of it. We detail a way to do that, under the assumption that a trusted beacon emits a uniformly random string in regular intervals. More specifically, the beacon, during slots $\{j \cdot R + 1, \ldots, (j+1) \cdot R\}$, reveals the j–th random string that seeds the leader election function. The critical difference compared to the static state protocol is that the stake distribution is allowed to change and is drawn from the blockchain itself. This means that at a certain slot sl that belongs to the j–th epoch (with $(j \geq 2)$), the stake distribution that is used is the one reported in the most recent block with timestamp less than $j \cdot R - 2k$.

Regarding the evolving stake distribution, transactions will be continuously generated and transferred between stakeholders via the environment and players will incorporate posted transactions in the blockchain based ledgers that they maintain. In order to accommodate the new accounts

that are being created, the $F_{LS}^{D,F}$ functionality enables a new (vk, sk) to be created on demand and assigned to a new party U_i . Specifically, the environment can create new parties who will interact with $F_{LS}^{D,F}$ for their public/secret–key in this way treating it as a trusted component that maintains the secret of their wallet. Note that the adversary can interfere with the creation of a new party, corrupt it, and supply its own (adversarially created) public–key instead. As before, the environment, may request transactions between accounts from stakeholders and it can also generate transactions in collaboration with the adversary on behalf of the corrupted accounts. Recall that our assumption is that at any slot, in the view of any honest player, the stakeholder distribution satisfies honest majority with advantage ε (note that different honest players might perceive a different stakeholder distribution in a certain slot). Furthermore, the stake can shift by at most σ statistical distance over a certain number of slots. The statistical distance here will be measured considering the underlying distribution to be the weighted–by–stake sampler and how it changes over the specified time interval. The security proof can be seen as an induction in the number of $\frac{L}{R}$ epochs with the base case supplied by the proof of the static stake protocol. In the end we will argue that in this setting, a $\frac{1-\varepsilon}{2} - \sigma$ bound in adversarial stake is sufficient for security of a single draw (and observe that the size of committee, m , now should be selected to overcome also an additive term of size $ln(\frac{L}{R})$ given that the lifetime of the systems includes such a number of successive epochs). The corruption delay remains at $D = R$ which can be selected arbitrarily smaller than L , thus enabling the adversary to perform adaptive corruptions as long as this is not instantaneous.

Stage 3: Dynamic state without a beacon, epoch period of R slots, $R = \Theta(K)$ and delay $D \in (R, 2R) \ll L$. In the third stage, we remove the dependency to the beacon, by introducing a secure multiparty protocol with “guaranteed output delivery” that simulates it. In this way, we can obtain the long–livedness of the protocol as described in the stage 2 design but only

under the assumption of the stage 1 design, i.e., the mere availability of an initial random string and an initial stakeholder distribution with honest majority. The core idea is the following: given we guarantee that an honest majority among elected stakeholders will hold with very high probability, we can further use this elected set as participants to an instance of a secure multiparty computation (MPC) protocol. This will require the choice of the length of the epoch to be sufficient so that it can accommodate a run of the MPC protocol. From a security point of view, the main difference with the previous case, is that the output of the beacon will become known to the adversary before it may become known to the honest parties. Nevertheless, we will prove that the honest parties will also inevitably learn it after a short number of slots. To account for the fact that the adversary gets this headstart (which it may exploit by performing adaptive corruptions) we increase the wait time for corruption from R to a suitable value in $(R, 2R)$ that negates this advantage and depends on the secure MPC design. A feature of this stage from a cryptographic design perspective is the use of the ledger itself for the simulation of a reliable broadcast that supports the MPC protocol.

Stage 4: Input endorsers, stakeholder delegates, anonymous communication. In the final stage of our design, we augment the protocol with two new roles for the entities that are running the protocol and consider the benefits of anonymous communication. Input–endorsers create a second layer of transaction endorsing prior to block inclusion. This mechanism enables the protocol to withstand deviations such as selfish mining and enables us to show that honest behaviour is an approximate Nash equilibrium under reasonable assumptions regarding the costs of running the protocol. Note that input–endorsers are assigned to slots in the same way that slot leaders are, and inputs included in blocks are only acceptable if they are endorsed by an eligible input–endorser. Second, the delegation feature allows stakeholders to transfer committee participation to selected delegates that assume the responsibility of the stakeholders in running the protocol (including

participation to the MPC and issuance of blocks). Delegation naturally gives rise to “stake pools” that can act in the same way as mining pools in bitcoin. Finally, we observe that by including an anonymous communication layer we can remove the corruption delay requirement that is imposed in our analysis. This is done at the expense of increasing the online time requirements for the honest parties.

Middlewares

DMChain dSSP (Decentralized SSP)

The decentralized SSP is the software of the network node. The ĐApp will use this software to conduct real-time advertising bidding for the advertisement and user interaction. The dSSP can be part of a ĐApp and can perform client functions as well as start on different network nodes. Different network nodes communicate through the dRTB protocol. The dRTB protocol defines that all parties use decentralized security to negotiate and execute profits in real time. The dSSP can store all transaction data in the dRTB event log store for subsequent analysis by publishers or audit providers in the event of a dispute.

DMChain dDSP (Decentralized DSP).

Decentralized DSP is software that bids through the dRTB protocol. DMChain provides its own dDSP implementation with a self-service interface module that allows advertisers to manage advertising campaigns. The DMChain dDSP will assist advertisers in adapting to the initial stages of the DMChain ecosystem. It is expected that traditional DSPs and trading platforms will use the dRTB protocol with their advanced positioning and optimization algorithms, and become more effective entry points for advertisers over time.

DMChain dDSP gateway

DMChain creates dDSP gateway software that enables traditional DSPs to connect to the DMChain ecosystem through a simple integration process and can use DMChain resources in parallel with their traditional advertising operations. To start the bidding, the traditional DSP needs to purchase the DMChain token to obtain liquidity and register as dDSP in the DMChain registration contract.

DMChain dSSP gateway

DMChain creates dSSP gateway software that enables traditional SSPs and ad networks to connect to the DMChain ecosystem through simple integration processes and gain additional inventory requirements. The traditional SSP will receive DMChain tokens for its traffic and will be able to convert it to other currencies if necessary.

DMChain auditor.

A key component of the DMChain ecosystem to enable fraud prevention in the dRTB protocol. In order to successfully achieve unprecedented transparency and security, the ecosystem will provide a special type of new market participants – auditors. DMChain will develop an auditor's open source basic implementation. Every DMChain participant who has a sufficient number of network resources to assess a large amount of fraud and other abnormal traffic will qualify as an auditor. These participants need to make an important security deposit in DMChain DAO and register in the audit register. In any negotiation, both the signing dSSP and the dDSP can use any registered auditor or even multiple auditors simultaneously to review the dRTB transaction flow. These auditors will act as third–party arbitrators to decide whether to adjust the transactions between users, publishers, dSSP and dDSP. As part of the analysis process, the auditor can provide participants with the following rankings:

- What is the probability that a user is an unbiased human?
- What is the probability that a user has forged his data?
- What is the probability that a publisher will breach an advertiser's brand security policy?
- What is the probability that an advertiser will breach a publisher's advertising policy?
- What is the probability that an advertiser will breach a user's advertising policy?

Typically, the transaction will be adjusted after a brief pause to allow the auditor to collect behavioral data about the participants in order to achieve a more accurate ranking. The aggregated data for all transaction flows will be signed by the parties concerned and used as the basis for DMChain's reputation management in the dRTB event log store. A flexible reputation mechanism will allow all ecosystem participants to make weighted decisions on bids when trading through dRTB. If participants exhibit inappropriate behavior, such participants will encounter scrutiny from potential partners, which may result in less traffic and fewer bids. With this setup, all participants get appropriate behavioral incentives and therefore enjoy greater market efficiency.

DMChain dDMP Gateway.

By providing APIs to compensate users for sharing data, DMChain opens up a fair and transparent market for DMP, collects, directs, and implements DMP as a commodity, and processes and presents it to data consumers such as dDSP, and these Data is monetized and generates

revenue. DMChain will implement a dDMP gateway library that uses the protocol to compensate for user data polling for subsequent analysis, integrates with traditional DMP, and simplifies its integration within the DMChain ecosystem.

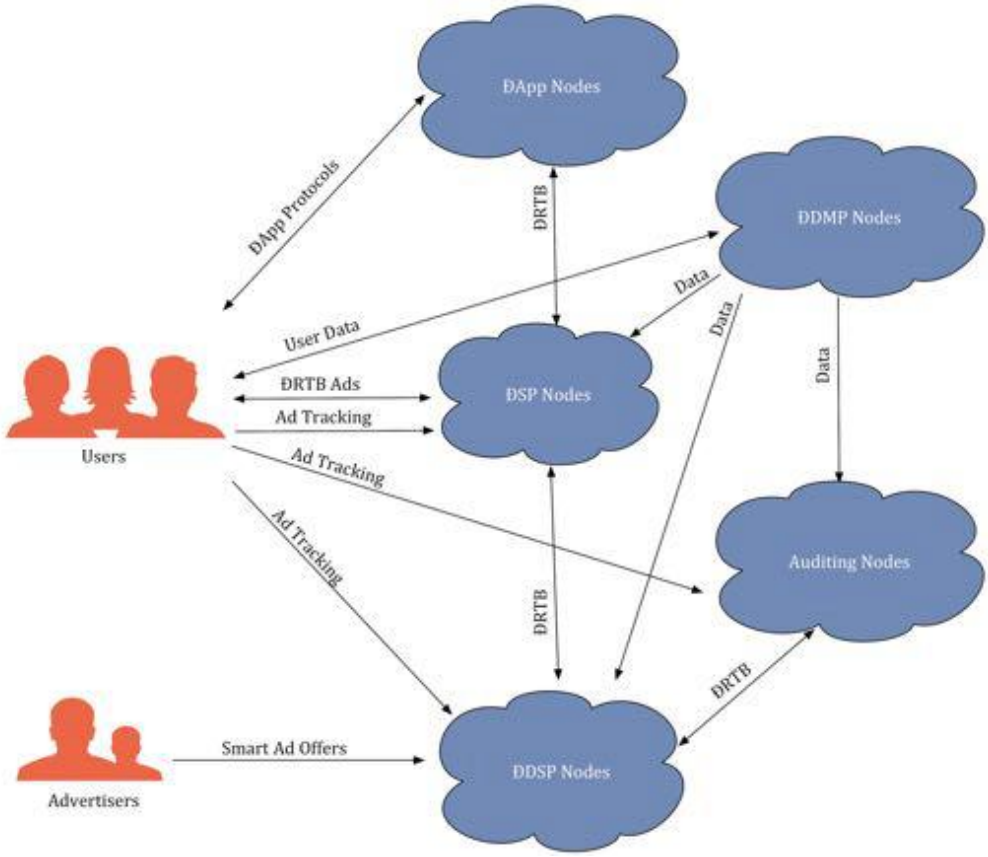

Figure 15. Interactions among DApps, middleware components, users and advertisers

Application Layer

The DMChain Infrastructure includes all components required to establish a complete digital advertising cycle within the DMChain ecosystem and to create gateways with traditional adtech systems.
On the basis of the three layers of DMChain architecture, developers will be able to build any kind of ĐApps with integrated advertising

monetization economies for use within the ecosystem. All ĐApps integrated with DMChain will constitute the 4th layer.

The SDK and APIs

- the encapsulation of dRTB protocol logic;
- the API for the integration of ad monetization models to ĐApps;
- the API for user data sharing with DMPs;
- the API for setting up and tuning data sharing policy, including balancing of data disclosure and appropriate user compensation;
- the API for setting up and tuning advertising policy, including balancing of ads exposure and appropriate user compensation.

The DMChain ecosystem will continue to provide upgrade software to support new ad formats within ĐApp. In the alpha version, DMChain will support simple banner integration and then add other formats such as video and native ads. ĐApp developers are free to use their own custom implementations and work directly with the dRTB protocol.

The ĐApps

DMChain will officially release a number of supplementary ĐApps for the ecosystem:

DMChain Account Manager for users. This ĐApp allows users to:

- register their identity and receive a DMChain ID;
- bind their cookies with DMChain ID to receive payments for ads displayed via DMChain on traditional websites and mobile apps via SSPs connected to DMChain using the dSSP Gateway;
- configure a personalized advertising policy — what ads a user wants to see and with what price;
- configure a personalized data policy — what data a user is willing to share, with whom and with what price;
- display statistics for ad and data interactions and receive profit;
- withdraw profits after identity verification to prevent Sybil attacks.

DMChain Account Manager for publishers. This ĐApp allows publishers to:

- register their identity on a publisher registry and receive a DMChain ID;
- create advertising integrations for their ĐApp and receive appropriate codes to begin using them in the ecosystem;
- configure advertising policy for each integration — what ads a publisher is ready to display and with what price;
- configure schemes of price distribution with users;
- display statistics for ad interactions, received profits and reputation;
- withdraw profits after identity verification to prevent Sybil attacks.

Content Check Proof of Stake / CPoS

In majority of digital advertising systems, payments are on the basis of clicks (CPM). When an advertisement publisher has displayed an advertisement or it has been clicked for a specific number of times, they get paid by the advertiser. Such an incentive mechanism is not in line with the original purpose of advertising and has led to various problems, since the CPM mechanism is a very weak indicator for the evaluation of an advertisement, where the number of times an advertisement is displayed does not equate with a good advertising performance.

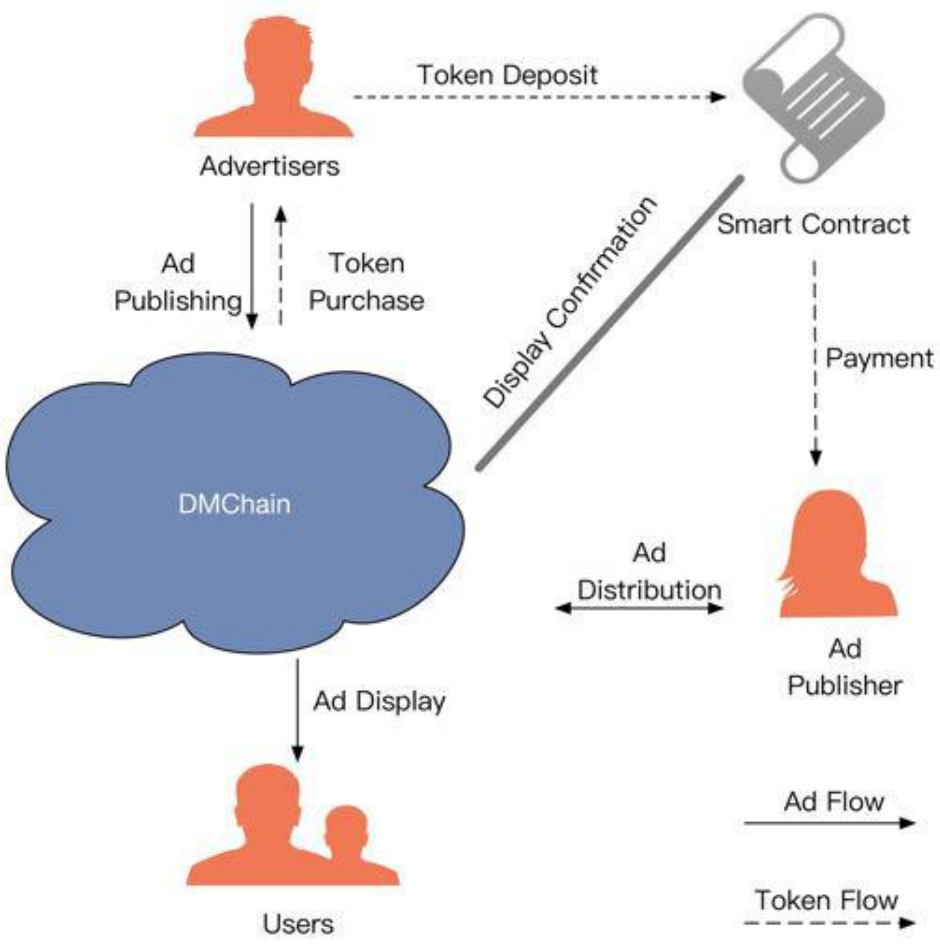

Figure 16. Incentive Mechanism

Technical Solution and Architecture

DMChain

In DMChain, we allow users to interact with the advertisements and we evaluate the performance of an advertisement based on the frequency and total amount of user interactions. Thanks to the transparency offered by blockchain technologies, DMChain can significantly reduce fraudulent activities in traditionally digital advertising platforms. In the meantime, since the interaction of users and advertisements is taken into consideration, advertisers will enjoy a much better advertising performance, in return attracting more and more advertisers to the DMChain.

Furthermore, since the payment and advertisement distribution process are automatically executed by smart contracts, trust between advertisers and publishers will no longer be an issue. It will thus facilitate fair competitions in the advertising industry and help building up a rigorous ecosystem. In order to encourage audience to interact with advertisements, they will receive a portion of the tokens as a reward. Distributing of the tokens help promote the token economy and make the stakes in underlying PoS system more distributed and more resilient to attacks. On the other hand, since users can freely trade the tokens the have received, it adds more liquidity to the tokens and can attract more users to DMChain.

Roadmap

2018 Q2 Complete design of decentralized digital advertising solution based on blockchain technology and publish white paper.

2018 Q3 Completed the first digital asset replacement of DMChain Token ADE.

2018 Q4 Build DMChain Ecology, and reach strategic cooperation with many blockchain media portals at home and abroad and from the media.

2019 Q1 DMNetwork Digital Advertising Network SDKs released, introducing media master participation.

2019 Q3 Smart Exchange-based DMExchange Digital Advertising Exchange.

2019 Q4 Released DMID DApp to introduce end users.

2020 Q1 PoS-based decentralized trading system.

2020 Q2 DMBaaS blockchain-as-a-service platform with three modules including DMSSP, DMDSP and DMDMP.

2020 Q3 DMChain digital advertising chain registered users reached 1 million.

2021 Q1 DMChain digital advertising chain exceeds traditional digital advertising platform.

2023 Q1 Completely decentralized DMChain digital advertising ecosystem completed online.

Our Team

Qingyun WANG Founder

Serial entrepreneur, technology believer. Rich, professional and practical experience in internet marketing. Well understanding of the marketing demand of company's each stage. In 2010, co-founded the second biggest domestic group-buying navigation website with millions of angel investment. In 2013, co-funded bitcoin trading website with investment from various institutional investors including Shenzhou pay and AAMA fund, one of top 5 bitcoin exchange in China, and set up branch in Japan, Australia. In 2015, funded digital marketing SaaS platform DMLei, devoting on resolving the difficulty of SME marketing and establishing new ecosystem of intelligent marketing.

Mingxing LU Operation Co-founder

Serial entrepreneur in internet industry. Mingxing joined a startup company in 2018 and had been independently responsible for back-end system development and project management. The company raised 40 million A round funding. Mingxing then founded KuLaDing Home Improvement O-to-O Platform, and seamlessly raised angel fund at early stage. The platform had its successful exit after getting acquired by Yuanzhou Home Improvement Group in 2015.

Our Team

Xiaole ZHAN Marketing Co-founder

Serial entrepreneur in media industry. Top 10 planning expert in 2014 and China Senior Business Planner. Xiaole once served chief editor for top news media in lighting industry, such as GZ Light Weekly, Chinese Pottery. His past endeavors also include publisher for Industrial Economic Review — a Chinese home improvement industry mainstream media, as well as general manager of newspaper center for for Xingbang Industry, Ltd.

Feng LI Technology Co-founder

Feng LI received his M. Eng. in big data and computer science from Peking University. 20-year experience in R&D and 10-year experience in technical management. He is the expert in the development of data mining and big data driven decision-making application.

Our Team

Polin Aleksandr System Architect

Polin has over 5 years of experience in software development and blockchain related research. He worked in consult.ru as the technical leader of private blockchain development for enterprises and was responsible for developing on-chain storage system. Polin is a enthusiast of blockchain and crypto technology.

Jirong TANG Advisor

Founder of S.Capital. Senior telecommunication expert and serial entrepreneur. Jacob served in Sail Investment Group and was responsible for FOF&VC investment. He has rich experience in equity and cryptocurrency investment in blockchain industry.

Our Team

Sun Zeyu Advisor

Founder of Creation Capital, co-founder of Kushen Cold Wallet, Consultant Member of Blockchain of Peking University Financial Technology Innovation Lab.

Tabitha Tao Resume Advisor

Senior marketing manager, MBA graduate from Simon Fraser University. Tabitha has deep understanding in digital marketing and brand management. She is good at planing and excuting social media marketing strategy on Facebook, Twitter, Youtube, etc,. Tabitha has more than 10 years online and offline marketing experience. While she served as brand manager in Cisco China, she is winner of Cisco CAP award for 5 consecutive years from 2004 to 2009 and nominator of Cisco APAC best marketing execution award in 2009.

Investor

Dawei HAN
DKB Founder
Yao Wei Capital Founder

Ding HAO
Coinbig Union Founder

Qianjie ZHAO
BTCC Senior　Vice President

Tuo TUO
HOFAN Managing Partner

Taiyang ZHANG
Coinmarket CEO

Junyu ZHANG
Encryption Vison Capital Founder

Investment institution

GENESIS 创世资本

S·Capital 一致资本

TIMESTAMP CAPITAL

Grand Shores

乐东资本 HAPPY EAST CAPITAL

浩方创投 HOFAN CAPITAL

金刚资本

天际资本 ZenithVentures

WEMEET CAPITAL 预鉴资本

Investment institution

DMChain

Blockchain Media Partner

Customer List (Partially)

Risk Statement

Risk of Lossing Access to Tokens Due to Loss of Certificate

Each buyer will have a corresponding DMC account prior to the allocation of ADE Token, and the only way to access the account is to use an associated login credential chosen by the buyer. The loss of requisite credentials will result in loss of such ADE Token. A proper way to store login credentials safely is to keep it away from any public place or a place where others have access to.

Risks Associated with the Ethereum Protocol

Prior to the launch of Cardano, because ADE Token and DMChain platform are completely based on the Ethereum protocol, any malfunction, breakdown or abandonment of the Ethereum protocol may have a material adverse effect on the Tokens or Platform, which, moreover, includes both the positive and negative effects on the price of Tokens.
For further information about Ethereum protocols, please visit http://www.ethereum.org.

Risks Associated with Buyer's Credentials

Any third–party that gains access to the buyer’s login credential or private key may be able to misappropriate one's ADE Token. To minimize the risk, buyers are expected to keep their electronic devices safe and prevent unauthorized access to their data.

Risks Associated with Uncertain Regulations and Enforcement Actions

Regulation on blockchain technology has been an important subject in many major jurisdictions. It is difficult to predict how or whether legislatures or regulatory agencies may implement changes to law and regulation affecting distributed ledger technology and its applications, including the Platform and the Tokens. Regulatory actions could negatively impact the Platform and the Tokens in various ways, including, for purposes of illustration only, through a determination that the purchase, sale and delivery of the Tokens constitutes unlawful activity or that the Tokens are a regulated instrument that require registration or licensing of those instruments or some or all of the parties involved in the purchase, sale and delivery thereof. Company may cease operations in a jurisdiction in the event that regulatory actions, or changes to law or regulation, make it illegal to operate in such jurisdiction, or commercially undesirable to obtain the necessary regulatory approval(s) to operate in such jurisdiction.

Risk of Insufficient Interest in the Project

It is possible that DMChain will not be used by a large number of individuals, companies and other entities or that there will be limited public interest in the creation and development of distributed Platforms more generally. Such a lack of use or interest could negatively impact the development of the Platform and therefore the potential utility of the Tokens, including the utility of the Tokens for obtaining Services.

Risks of Failing to Meet the Expectations

The Platform is still under development and may undergo significant changes prior to the final release of a stable version. There is a risk that the Tokens or Platform, as further developed and maintained, may not meet community or users expectations at the time of purchase. Furthermore, despite Company's good faith efforts to develop and participate in the Platform, it is still possible that the Platform will experience malfunctions or otherwise fail to be adequately developed or maintained, which may negatively impact the Platform and Tokens, and the potential utility of the Tokens, including the utility of the Tokens for obtaining Services.

Risk of Hacking and Theft

Hackers or other malicious groups or organizations may attempt to interfere with the Platform or the Tokens in a variety of ways, including, but not limited to, malware attacks, denial of service attacks, consensus–based attacks, Sybil attacks, smurfing and spoofing.

Risk of Continuous Development of Cryptography

The rapid development of cryptography, and/or the development of computing technologies, such as quantum computers, will bring unprecedented risks to the use of cryptocurrencies and DMChian community, and possibly result in loss of tokens.

Risk of Lack of Maintenance or Use

Although tokens should not be seen as an investment, they will have some value on the cryptocurrency market. However, if there is an insufficient use or maintenance on DMChain, this value may be reduced. In such case, the Platform may not have enough participants or users, so the Tokens may be impacted negatively.

Risk of Uninsured Losses

Unlike bank accounts or accounts at some other financial institutions, Tokens are uninsured. Thus, in the event of loss or loss of utility value, there is no public insurer, such as the Federal Deposit Insurance Corporation (FDIC), or private insurance arranged by Company, to offer recourse to you.

Risk of Dissolution of the Company or Platform

It is possible that, due to any number of reasons, including, but not limited to, an unfavorable fluctuation in the value of ADE Token, decrease in the Tokens' utility (including their utility for obtaining Services), the failure of commercial relationships, or intellectual property ownership challenges, the Platform may no longer be viable to operate or the Company may dissolve.

References

[1] Nakamoto S. Bitcoin: A peer-to-peer electronic cash system.

[2] Buterin, V., 2013. Ethereum white paper. GitHub repository.

[3] Kiayias A, Russell A, David B, Oliynykov R. Ouroboros: A provably secure proof-of-stake blockchain protocol. In Annual International Cryptology Conference 2017 Aug 20 (pp. 357-388). Springer, Cham.

[4] Van Deursen, A. and Klint, P., 2002. Domain-specific language design requires feature descriptions. Journal of Computing and Information Technology, 10(1), pp.1-17.

[5] Borthakur, Dhruba. "HDFS architecture guide." Hadoop Apache Project 53 (2008).

[6] Siegel, J. ed., 2000. CORBA 3 fundamentals and programming (Vol. 2). New York, NY, USA:: John Wiley & Sons.

[7] Davenport, Shaun, and Richard Ford. "SGX: the good, the bad and the downright ugly." Virus Bulletin (2014): 14.

[8] Klomp, Jeroen van Leur Jeroen. "Recursive InterNetwork Architecture." (2016).

[9] Lamport, Leslie. "On interprocess communication." Distributed computing 1, no. 2 (1986): 86-101.

[10] Mullin, Lenore MR, and Michael A. Jenkins. "Effective data parallel computation using the Psi calculus." Concurrency: Practice and Experience 8, no. 7 (1996): 499-515.

DMChain

Decentralized Digital Advertising Platform on Blockchain

Whitepaper3.0