BRAHMA OS

TECHNICAL WHITE PAPER

VERSION 1.0

http://brahmaos.io/
@BrahmaOS
@brahma_os
https://medium.com/brahmalabs

Brahma OS Technical White Paper

Version 1.0

February 27, 2018

Abstract

Brahma OS is an operating system that supports decentralized networks with the deconstruction of existing services and the use of various decentralized services and components, which ensures that users can make use of services and applications on the blockchain safely and easily.

Contents

1 Background

Blockchain technology is known through the birth of bitcoin in 2008. Since then developers and entrepreneurs have been experimenting with this technology in hopes of using it in a broader range of products to solve the technical pain points in different area of industry.

However, blockchain technology is not a technology that solves technical pain points in the existing corporate structures. Instead, it works on a self-governing and non-central value network to sustain a safe, continuous operation of the network through incentives mechanism.

Ethernet brings the potential for non-stop applications with the smart contract architecture. In a short year of 2017, revolutionary solutions and implementations such as the Kyber Network, 0x Protocol, and Radian Network emerged over the Ethernet, bringing the prospects and expectations of non-center application to the future.

At the same time, other public chains which can carry applications is also emerging, such as EOS or ADA. However electronic devices such as the mobile phone which has the most significant number of users and which takes most time of the users, still runs on an OS that relies on a central server, from user account systems to personal data backups, then to building application logic on OS. Apparently, the existing OS does not provide a foundation for the future application of the blockchain.

2 Requirements of decentralized OS

Unlike iOS and Android OS, decentralized OS requires complete removal of the architecture design of the central server at the beginning, from basic services to upper-level

application achitecture. While ensuring the usage habits on the UI / UX level as much as possible, we pay more attention to the function and the value that central services can play in the OS.

2.1 Data privacy

When using an OS, it is valuable whether the data is intentionally generated by the user or by an inadvertent operation.

Such data forms the basis of artificial intelligence analysis and is called factual data. With the same factual data, different user portraits can be generated when data mining algorithms are optimized. Moreover, all the personalized services we know today, such as online shopping recommendations, friend recommendations or voice recognition, rely on user portraits generated by factual data. These factual data of billions of users made it possible for the commercial empire like Facebook or Google to be established.

However, in the commercial closed loop of centralized services, users contribute their actions and factual data but do not get financial reward. These data can be sold again and again. In a way, business models for systems and App vendors are now mainly based on the user privacy data without giving financial rewards to the user.

In Brahma OS, privacy issues could be fundamentally solved. Stealing and exploiting user privacy data would become very difficult to perform.

2.2 Accessible network communication

Whether in the blockchain field or the current Internet economy field, network communication connections are issues that need to be solved first. How to access to data on the web at any time becomes a crucial issue.

When we talk about network communications, most of the time we are talking about

how the terminal connects to a wide area network. In the current architecture, the terminal device connects to the meta-network (i.e., the local area network to which it can connect directly). Then meta-network connects to different meta-network or the upper network through the router and switch. Most of the connections between different meta-networks are current operators. From this, we can have two layers: network and router.

The end nodes in the meta-network can form a peer-to-peer network, that is, the nodes in any meta-network are offline and should not cause unreachable communication in the meta-network. This is not the core of our concern, as its connectivity problems are not hard to solve. The critical problem goes to the router.

In current network communications, we must trust and can only trust the router. In fact, the router not only can completely intercept and spy on the data, protocol, and trend of communication between meta-networks but also act on it, such as tampering the service and denying the service.

In currently available network communications, OS end-users face two major problems: privacy exposure, unprotected accessibility.

Therefore, in the Brahma OS, we expect to build a peer-to-peer OS network to ensure the encryption of the communication data and the non-identifiability of communication data through protocol confusion at the data transport level, and to build an autonomous connected network based on the configuration of the routing.

2.3 Decentralized Storage

Today, most of the OS provides users with the fonction of cloud storage. Users in different devices only need to log in to the same account to access the same data. Cloud storage brings users personal conveniences. At the same time, there are some potential problems with personal data security.

Dropbox loopholes lead to loss of personal data. Nude photos of some celebrities were leaked when their iCloud accounts were attacked by hackers. Issues like th??se reveal an apparent problem: in the current centralized cloud storage architecture, It is only a matter of time before the security problem is revealed.

Decentralized chain storage avoids this kind of problem from the very beginning of the design. Taking IPFS as an example, the decentralized storage has no server that can be attacked or be traced. All data are divided into multiple parts, randomly stored in different nodes of the network. The entire network is safe and efficient for storage and transmission thanks to miners in storage networks.

When building storage services, Brahma OS uses directly decentralized web services. For now, we do not guarantee the use of IPFS. We would compare other potential decentralized storage services like Sia, Storj, and MaidSafe as well.

2.4 Cryptographic assets management

Asset management is a function need to be completed at the wallet application layer. We consider this demand from the OS's perspective. In the foreseeable future, cryptographic assets would be less dependent on centralized exchanges. The role of centralized exchanges transforms from the current speculative trading into connecting blockchain assets and legal assets. Cryptographic assets exchange can be fulfilled with decentralized services.

Now, based on the backbone of Ethereum, we can provide service by building transaction relayer with the 0x protocol. This protocol can connect all the other built replayer. That is, this protocol does not only provide liquidity within a single application but the asset liquidity among all replayer.

Another possible way is through Kyber Network. Unlike Ox, Kyber Network it-

self can serve as a decentralized exchange. An exchange or convert request can be executed immediately within a single transaction without a relayer.

Compared with available options of exchange service, it is necessary to construct exchange service from the OS-level. Brahma OS can be the carrier of many D-Apps. All consumption in D-App should be on-chain (rapid transactions off-chain would be on-chain eventually). In the process of a transaction, a payment request can be initiated by a D-App and can go directly to an end-user.

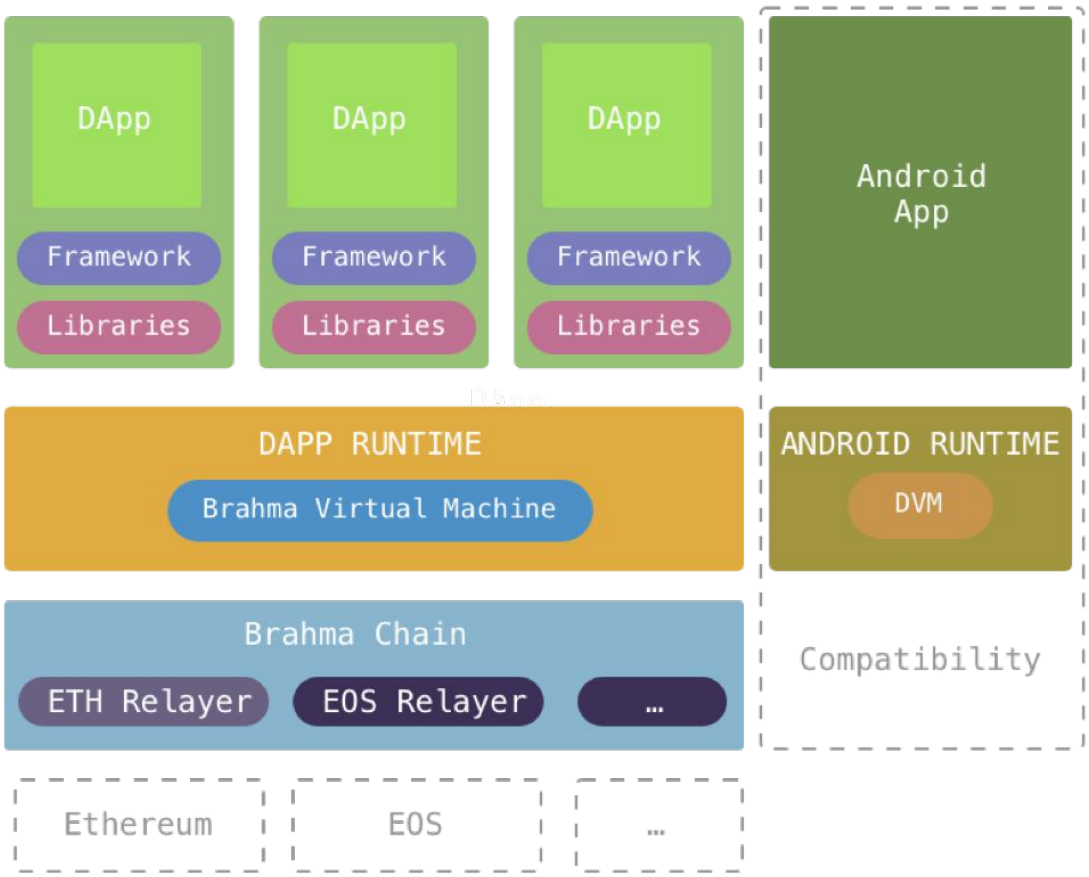
2.5 Autonomous economic system

From last year, there have been significant technological breakthroughs on Ethereum. These breakthroughs bring closer the distance between the blockchain and users.

In the initial stage, Brahma OS provided autonomous unobstructed network communication service and foundation of the upper application services by integrating technical solutions such as IPFS, Kyber Network, and 0x. With the cross-link technology and Brahma OS backbones, we will build a complete ecosystem based on the Brahma OS chain that connects other backbones such as ETH, EOS, and ADA.

3 Architecture

3.1 Layered design



Brahma OS uses a layered design scheme to stratify Chain, Runtime, and Framework. Taking into account the Android native application compatibility issues, we separate the Virtual Machine so that Android App runtime environment and D-App runtime environment are entirely isolated, and to ensure that, even if there is dangerous behavior, Android App cannot get any information from D-App.

Brahma Virtual Machine (BVM) is specially designed for D-App in Brahma OS for its op??ration and for the operation of its associated framework and Libraries.

Brahma's independant chain works as a Chain Context. It is expected to serve as an intermediary role to connect other application chains (such as Ethereum, EOS, etc.) through Chain Relayer.

3.2 Consensus algorithm

As an independent blockchain, Brahma OS Chain's consensus algorithm is crucial to data security. Currently, we mainly consider two possible projects: DPoS and DAG.

DPoS was originally proposed by Bytemaster and used in BitShares, Steemit and EOS. Its main features are higher TPS (TX per second) and at lower consensus maintenance costs. In contrast to the PoW consensus competition mechanism, DPoS tends to reach a consensus with the collaboration of Witness node.

DAG is a graph in graph theory. In the beginning, IOTA attempted to replace the existing blockchain structure with DAG to provide a value delivery network through mathematical proof rather than through consensus mechanism. After IOTA, there are other projects such as Byteball which proposed improvements of DAG. The main feature of DAG is the ability to deal with transaction requests at higher concurrency without block structure and therefore, no limit to TPS.

3.3 Compatibility and security

We believe that decentralized OS will eventually replace the current centralized OS. That requires not only time and effort of users but also their learning process. That is why, at the beginning of the design, we take both compatibility and security into consideration.

The existing Android OS is relatively complete. Therefore we consider providing a runtime environment with Dalvik Virtual Machine for the existing Android App while working on the related products of Brahma OS (such as Brahma Virtual Ma-

chine and Brahma Chain).

In this way, we guarantee the compatibility of our product and at the same time, we isolate the interaction between the Android App and the D-App at the runtime level, thereby avoiding the possibility that the Android App steals the key and information from the D-App.

4 Identity

Identity is the primary element in any system and the premise of logical interaction and functional interaction between man and machine.

In Brahma OS, the identity is no longer dependent on the centralized service account system, but directly use the blockchain public key as the the user identity to connect to the entire decentralized service system.

4.1 About "I"

The reason why we will give up the centralized service account system is mainly based on our understanding of the identity of "I" in the entire network architecture.

In current centralized account system, end users need to register to get a distributed identity from a centralized service provider. This identity authorizes the user to log in to the system for the follow-up operation, which brings several problems:

- When switching between different account systems, the data of "I" do not interwork with each other.
- "I" is redundant in different accounts and not mutually exclusive.
- All factual data and user portrait generate by "my" act can be easily obtained at no cost by a centralized service provider.

In summary, "I" is authorized to access in current centralized network and its factual data is unconditionally deprived.

When the password of an account is leaked or the service provider is hacked or user's personal data, "I" becomes powerless.

4.2 Role and value of identity

Based on our perception of "I", i.e. identity, we know that, identity, as an access token to the system, is linked to a set of business logic. The identities built on the central service providers are isolated, redundant, non-cross-linked and insecure. However, user's identity is a valuable resource and barrier in the current Internet economy. Therefore, returning the value of identity to the user is important for Brahma OS.

Through the above description, we can see that identity, in a complete system, plays two roles:

- get account system authorization
- access and operate the account system

In Brahma OS, identities plays other roles:

- asset identification
- user portrait
- user portrait D-App match

Brahma OS expects to offer users the opportunity to collect user factual data at the OS level and to train their AI for the perfection of user portraits. When D-App needs to use these user portraits, it pays directly to the user to ensure that the final revenue belongs to the owner of the OS, not to any intermediate role.

4.3 Significance of decentralized storage

Decentralized storage of user-related data can be more valuable than other centralized cloud storage.

We talk about several disadvantages of centralized cloud storage:

- It exists systemic security risks in centralized systems.
- Cloud storage service providers do not share identity information.
- Any centralized cloud storage service providers' compromising will threaten other service providers

At the beginning of designing the decentralized storage, we avoid such kind of problems. Even if the key is stolen due to personal or other reasons, the leakage of personal data will not cause the loss of other user data in the system.

At the same time, the user's identity is no longer the source for commercial companies to get user's personal information. All fees will go back to the user himself. The problem of requiring centralized storage and processing of user's data was circumvented from the very beginning. Everyone holds their own data which distributed discretely in a decentralized storage network. No one (organization) can monitor the whereabouts and content of personal data or hijack user data. This will bring a lot of possibilities for protecting personal data privacy, the behavior freedom, and the value return. It is the basis for reshaping the existing business model.

5 Network

Network connectivity will eventually be accessible without barrier.

5.1 Role of network

In Brahma OS's network, we can ensure network connectivity and autonomous economic construction in different ways. Here, we distinguish the way of meta-network nodes and routing network nodes.

5.2 Construction of meta-network

Meta-network is the smallest unit of a local area network.

In the meta-network, different nodes are peer-to-peer with each other and do not need additional traffic costs. Therefore, the construction of meta-networks mainly occurs in a small area. The interconnection between devices at a short distance can be achieved directly through Bluetooth and other protocols.

Brahma OS can be interconnected to build a meta-network and diffuse as a minimum unit. When sending data in the meta-network, the application layer protocol itself will do many obfuscation measures; the data will be fragmented, encrypted to ensure that the data transmission in the meta-network will not leak data content.

5.3 Routing

Routing can connect to different meta-networks and the upper WAN.

Multiple routing can form a meta-network structure. They provide data exchange services between different meta-networks to form a non-central traffic market.

In Brahma OS, routing nodes which connect to different meta-networks can provide traffic exchange between different meta-networks or between meta-networks and wide-area networks. Thus, a device as a routing node can obtain some economic return as well.

6 Application basis

The purpose of Brahma OS with decentralized services is to provide a foundation for applications. D-App developers do not need to put too much effort into how to get decentralized services but to focus on how to construct application logic.

6.1 Runtime environment

The Brahma OS runtime environment runs as a sandbox environment for Native D-App. We should ensure:

- complete isolation
- executive efficiency
- decentralized component of the calling environment

Complete isolation provides safe running space for D-App. "Security" in this context means not only that the data of a App itself cannot be infringed, but also that the operation with other App is isolated from each other.

As a Native App, the efficiency of execution is crucial, which is directly related to the quality of the user experience. At the system's priority level, Brahma OS preempts transactions related to user interaction while network-IO-related execution runs in parallel in the background.

6.2 Application structure

The D-App above Brahma OS should include two key components: Brahma OS services components, UI components.

6.3 Decentralized service components

As mentioned above, many decentralized services above Ethereum are being introduced. For developers, how to interface with best practices is crucial. It affects not only development progress of D-App but also user's asset security or other issues.

Therefore, Brahma OS is expected to provide developers with:

- components SDK for quick integration
- rich documentation
- best practice access sample
- actively involved developer community

For example, when a user in a D-App needs to purchase an item using ETH, he no longer needs to go to the wallet to start a transaction. Instead, he use Brahma OS's payment component in the game to show the payment request information to the user. User's perspective will also change from the transaction logic in the past to the payment logic. It brings possibilities for a wider use of cryptographic assets.

6.4 D-App store

In addition to bringing a lot of technological breakthroughs, Brahma OS brings a huge possibility for next new ecology, D-App Store.

Unlike App Store or Google Play, we expect D-App not to be a centralized operator, but a decentralized market where users are directly involved in operations. New business models can build on it. For example, the revenue from D-App can

directly go to the rating users or recommended users without any intermediate role to deprive D-App's revenue.

7 Conclusion

Brahma OS is stepping into a whole new area which cryptocurrency has never touched before. It will act as the central role in connecting end-users to the blockchain network. It not only integrates many of the existing decentralized services but also provides its developers with an infrastructure and a complete ecosystem to quickly build applications. It shows an important advance in the exploration of blockchain technology.

Moreover, since user-identity data is no longer divided into different central systems, different D-Apps can be more personalized based on the same user identity. Developers can find users that meet their target audience by paying the D-App Store's recommender system. These users can receive payment directly. At the same time, it could promote a higher conversion rate of D-App.

8 Roadmap

Phase 1 Token exchange

2018 Q1

- Token exchange and token distribution

Phase 2 MVP

2018 Q2-Q4

- Remove Android centralized service component
- Set schedule for further development of decentralized service component
- Access ethernet network
- Adapt key models
- Make preliminary running test of Brahma OS

Phase 3 DEX Integration

2019 Q1

- Complete decentralized tokens exchange service
- Test decentralized token exchange

- Confirm the package of decentralized token exchange

Phase 4 Decentralized backup service

2019 Q2-Q3

- Complete decentralized storage service
- Test decentralized storage services
- Package decentralized storage services and decentralized components

Phase 5 Brahma blockchain research

2019 Q4

- Design consensus model and virtual host running model
- Test and compare consensus program

Phase 6 Brahma blockchain testnet

2020 Q1 - Q2

- Test Brahma chain consensus mechanism
- Test Brahma Virtual Machine
- Deploy Brahma testnet

Phase 7 D-App and Brahma D-App store

2020 Q3 - Q4

- Reconstruct the upper D-App architecture
- Improve D-App development framework project
- Improve toolchain development
- Design and improve D-App store architecture and integrated distribution project

Phase 8 D-App Developer community building

2021 Q1

- D-App hackthon
- Support excellent developer
- Host technical salon for core developer

Phase 9 Ecological construction and foundation

2021 Q2 - Q4

- Foundation invests in D-App and core components construction project
- Negotiate business cooperation with more industries
- Enhance Brahma OS's influence
- Start the Brahma OS DevCon project

9 Token Exchange

- Expected minimum amount: 60,000 ETH
- Expected maximum amount: 80,000 ETH
- Total circulation: 3,000,000,000
- Proportion of the transfer: 40
- Purpose of the remaining proportion: to be determined