Next Generation High Performance Blockchain Game Platform

Pure Distribution, Safe & Reliable

Efficient & Easy Deployment

Version 0.1.0

February, 2019

Abstract

The blockchain technology represented by Bitcoin and Ethereum is building a new, more equitable, transparent and credible Internet world with a dramatic trend of reforming. However, there is not yet a blockchain consensus mechanism that perfectly balances the “decentralization, security, and scalability” (Blockchain Trilemma) at present. In practice, it encounters different levels of technical bottlenecks. Kaleido is born for achieving this breakthrough and bringing blockchain technology to large-scale commercial applications.

Kaleido is positioned in the high-performance blockchain game application platform with a core consensus mechanism based on verifiable random algorithm - Algorand, which aims to achieve higher degree of security, higher performance extensions of distributed applications and higher decentralization of blockchain underlying chain, thus providing a new technology solution for breaking through the "impossible triangle". We designed a purely distributed blockchain game architecture based on VRF, making full use of blockchain open account book, cryptography verification mechanism, P2P trusted network and other technologies to achieve a truly decentralized application development, endowing game fairness, transparence, and trustworthiness. At the same time, based on the Algorand consensus mechanism that any node can freely enter and exit and

permission contract mechanism designed for the game contract, the game complexity and experience can completely reach those of current centralized server.

Through practice testing, we built a permission contract mechanism based on system contract to effectively resist DDoS attacks. Also, users do not have to pay the gas fee, meaning that those who do not hold the token on chain can easily apply dApps. This innovative technology can vastly expand the incremental users of dApps and make blockchain applications for billion-level users truly possible.

CONTENTS

1 Background 6

1.1 Pain Spots of Game Market 6

1.2 Kaleido Solutions 11

1.3 Kaleido Design Principles 17

2 Kaleido Technical Solutions 23

2.1 Kaleido Overall Collaboration Architecture 23

2.2 Kaleido Basic Tech Units 25

3 Algorand Consensus Mechanism 26

3.1 Strengths of Algorand 27

3.2 Execution of Algorand 30

3.3 Token Circulation Model 37

4 Trustworthy P2P Network 40

4.1 P2P Network Communication Mechanism 40

5 Game Script Driving Framework Based on Trustworthy P2P Network and Smart Contract 41

6 Open Encrypted Account 42

6.1 Homomorphic Encryption 42

6.2 Zero Knowledge Proof 43

7 Privilege Control Contract Mechanism Based on Smart

Contract..... 44

8 Kaleido Application Scenario 46

9 2019 Annual Development Plan 47

10 Conclusion 48

References..... 51

1 Background

1.1 Pain Spots of Game Market

- The Infrastructure: Main Bottleneck for Large-scale Blockchain Landing

Since the birth of Bitcoin in 2008, the blockchain, as a distributed public accounting technology based on P2P transmission, has realized decentralized peer-to-peer transactions in distributed systems where nodes do not need to trust each other, thus solving the high cost, low efficiency, insecure and untrustworthy data storage and other issues of centralized organizations. Also, blockchain introduces value transfer and distribution mechanisms, which kicks off the value transmission network.

In the underlying foundation of blockchain, the public chain, Bitcoin controls the absolute superiority of the PoW (Proof of Work) consensus mechanism. In the past 10 years, the world's increasingly powerful computing power has escorted the security and stability of this system, but the trend of centralized

monopoly, low performance and high energy consumption are also not suitable for large-scale commercial use. Based on this, the PoS (Proof of Stake) consensus mechanism is proposed to replace the computational workload proof with the economic interests of the participants, thus balancing the shortcomings of performance, in which DPoS（Delegated Proof of Stake）, represented by EOS, tries to further improve system performance at the expense of decentralization. However, the recent hacking incidents have exposed the shortcomings of security.

It can be clearly seen that there is an “Blockchain Trilemma” in the consensus mechanism of blockchain technology. At present, there is no consensus mechanism that has already landed to balance the relationship between performance, security and decentralization. If blockchain technology aims to achieve large-scale commercial application, it must meet these three requirements.

In the application progress, the dApps currently developed based on the smart contracts of Ethereum, EOS and other public chains are mostly games. Because the smart contract is a public ledger

on the chain, the operation of the game needs to be done on the chain. Limited by the operational performance and cost of smart contracts, the current blockchain game is not complex and the user experience is not good enough. On the other hand, the operation of large games requires high concurrency, zero delay, fluent and sensitive interaction, but the existing performance of public chain is far from meeting this requirement.

In addition, the existing public chain is too hard for developers to get started. Though the cost of ETH's deployment of dApp only lies in contract development, but ETH TPS is far from the requirement of large-scale commercial use. EOS developers need to purchase the underlying technical resources and bear the running costs. It is even more difficult to develop dApps due to supporting tools, programming languages, etc. Thus, the game types of ETH are relatively more diversified than EOS’s, whose basically are only gambling games. However, in view of the fact that many dApps require high TPS, most application developers can only choose EOS, which is the least of two evils, not the best of two options.

- Existing Blockchain Game: Hard to Play

On the one hand, the operation of dApp requires cumbersome steps such as downloading a special wallet and pre-charging the cryptocurrency, also it involves the preservation and security of the private key. For most audiences who are not familiar with the blockchain, the cost of marketing education is vast. On the other hand, in games that rely on certain public chains such as Ethereum, most of the chain interactions need to consume transaction fees which is a high cost for players and greatly affects the experience. To a certain extent, these have led to the current low activity of the blockchain game dApps, the small amount of user coverage, the difficulty of forming a scale effect, hence hinder the commercial landing process of blockchain technology.

At present, the advantages of blockchain games are not intuitive, and the experience is not comparable to traditional games. Only pyramid sales mode can be spread in order to attract users which leads to a very short game life cycle and an extremely limitation to speculative users of the cryptocurrency, totally unable to be extended to traditional players with a larger volume.

- Traditional Games: Obvious Drawbacks for Developers and Players

Traditional games run on centralized servers which bears a high technical safety risk. First, the games running on the centralized server are at risk of being banned and stopped at any time. It is a high loss for both game developers and players; Second, centralized server games often face hackers, DDoS and other technical attacks; in addition, the monopoly of traditional game makers is obvious, small and high-quality game developers are difficult to guarantee their survival and benefits, which means the risk of game development is extremely huge for them.

On the other hand, in the era of Internet games, gamers and developers tend to stand on the opposite side. The game mechanics and numerical algorithms in the centralized game are opaque. The ownership of virtual assets such as equipment, skin, mounts, etc. does not belong to the user but belongs to the game manufacturer. Real assets only flow to the virtual assets in one direction, which leads to the closure and non-circulation of the

intrinsic value of the traditional game. In addition, the in-game economic system also has a tendency to hyperinflation due to the continuous increase of virtual currency, therefore the interests of players cannot be guaranteed.[1]

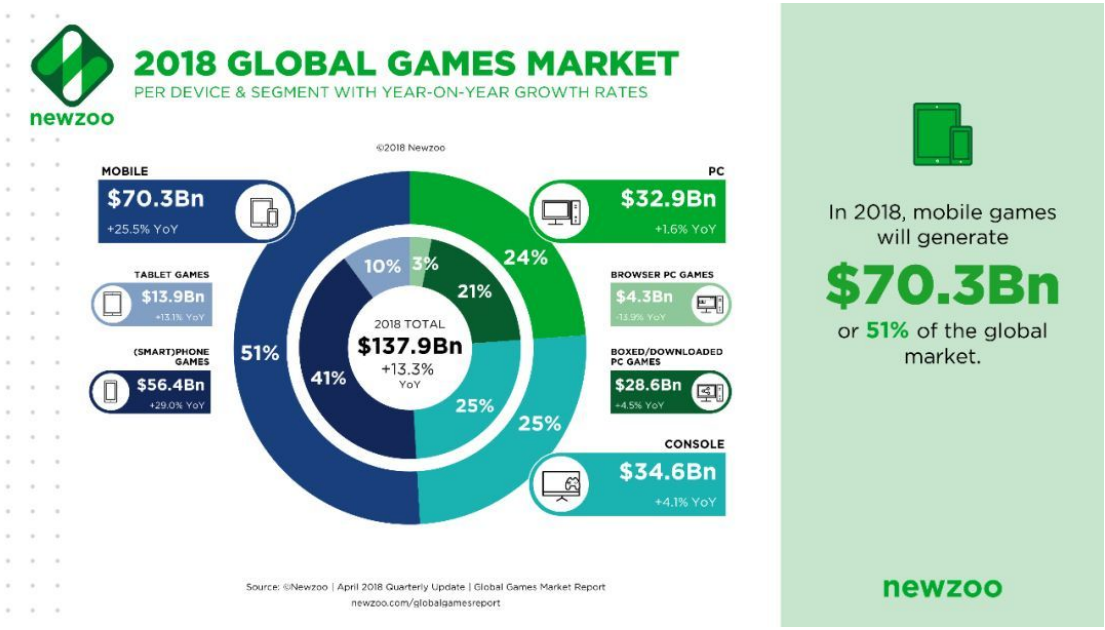
1.2 Kaleido Solutions

As far as the application scenario is concerned, the most suitable application field for blockchain technology is native digitization, rather than a huge connection with reality. The blockchain is more suitable for: areas with low communication efficiency and high cost of trust; areas that have great demand for authenticity and consensus (more common in opaque, black box operations); areas with long tail flow, resource dispersion, and imbalanced interests among ecological participants. The digital game industry is undoubtedly an important tipping point for the blockchain to move towards the public.

According to relevant statistics, the global game market reached US$137.9 billion in 2018, with more than 2.3 billion gamers worldwide, accounting for one-third of the world's total

[1] References: "Huobi Blockchain Industry Special Report: Game".

population[2]. China accounted for more than 25% of the global game market, reaching US$37.9 billion. The Asia Pacific gaming market is over 52%, reaching $71.4 billion. The game audience tends to be young and acceptable for new things, which is in line with the characteristics of the new technology such as blockchain, and is expected to form a strong fusion force in the future.



1.1 2018 Global Games Market

More importantly, the transparency, fairness and credibility brought about by the blockchain game will greatly change the

2 Source: Game Market Research Company Newzoo, "2018 Global Game Market Report".

problem of numerical opacity, black box operation and a series of centralized risks. Through technology and token fuel, the interests of game manufacturers and the players' community will be highly consistent, and players will regain a purer game experience and the ownership of game assets, loyal players will spontaneously maintain the balance of the game, introduce more innovative play types and experiences, help manufacturers acquire users and prolong the life cycle of the game. This fair and transparent mechanism and community consensus based on co-construction and co-prosperity will surely lead to the prosperity of the whole game industry.

In view of the existing problems of blockchain and the traditional game industry, we construct a blockchain P2P technology network architecture for the game field, which enables complex games to truly land on the blockchain. This architecture makes full use of open and non-tampering account technology, cryptographic authentication mechanism, and P2P network to achieve the deployment of truly decentralized game applications, and has excellent performance, so that the complexity and experience of the game can reach the current level of traditional

centralized servers. At the same time, it greatly improves the fairness, transparency and security of online games.

Kaleido solutions are as follows:

1. Kaleido introduces a brand-new consensus mechanism upgraded from pure PoS（Proof of Stake）: Algorand. This algorithm combines the advantages of VRF and PBFT, and creates a random lottery election method to achieve greater fairness and decentralization. It aims to build a distributed account book with low energy consumption, high speed, democratization, good scalability and low bifurcation rate, and solve the "impossible triangle" problem in the existing blockchain consensus algorithm. Node participation does not require any permission, anyone who owns equipment can participate in accounting as a node, and does not need to consume too much computing resources. Under this algorithm, each node is equal and can easily extend to millions of nodes. At present, the existing consensus algorithm based on PBFT can only be applied to alliance chains of dozens to hundreds of nodes. The TPS of the Kaleido test network is currently stable at around 3000, with an average of 2 seconds to

block out. Once block out, the transaction is finally confirmed. It is expected that once the main line gets on line, the target TPS will reach up to 5000.

2. Kaleido greatly extends the chain function and designs a new dApp application development mode. Besides compatible with the development environment and inheriting the friendliness of Ethereum to developers, we also extend more on-chain functions: besides publishing accounts, we also provide the function of automatically establishing P2P application network, which enables applications to directly establish a trusted P2P network on the chain, and complete the exchange and transmission of messages in this network, thus enabling the application data between each node can be transmitted and invoked fairly and openly, which will greatly expand the landing scenarios of applications on chain.

3. Kaleido greatly protects the high privacy of game data by publishing double-encrypted accounts. Although blockchain cryptography achieves anonymity of transaction subjects, one of the major challenges for the application of blockchain

cryptography in game industry is the privacy of transaction content (including transaction volume, transaction time, etc.). Whether it's ETH or Bitcoin, the trading content and account balance on the chain are open to everyone. For developers and players in the game industry, they are more sensitive to the data link of the game transaction and do not want the trading content to be disclosed. Based on this, Kaleido specially designed a double-encrypted book-keeping mechanism. By applying homomorphic encryption and zero-knowledge proof technology to the current intelligent contract, two kinds of public encrypted books were realized, one is the encrypted token contract corresponding to ERC-20 token, the other is the encrypted settlement book based on game application, which guarantees the high security of system data and the protection of user privacy.

4. Kaleido implements a system contract-based privilege contract mechanism for game contracts. Through this privilege contract mechanism, dApps can effectively control the access account of the contract, thus increasing the possibility of resisting DDoS attacks. At the same time, through this mechanism, contract

accounts can be used to pay gas fees instead of users, so that users without token on the chain can participate in the experience of dApps, which can greatly expand the coverage of dApp users, thus making it possible to apply the blockchain to the general public.

1.3 Kaleido Design Principles

In order to achieve large-scale commercial applications, blockchains must meet the high requirements of "de-centralization, security and performance". Based on this original principle, Kaleido aims to build a distributed trust network with high security, decentralization and support for ultra-large-scale applications. The design principles are as follows:

1. Genuine Pure Distributed Network

Based on Algorand's VRF+PBFT algorithm logic, each new block is voted by an independent committee, which is randomly drawn from all user sets. In the election of the committee, VRF (Verifiable Random Function) is introduced to make the election of consensus committee and block proposer completely

unpredictable, and to make each round of consensus process executed by block proposers and committee members different. Each node has the right to participate in the encrypted lottery and generate new blocks. The weights in the lottery are proportional to the account balance, which is similar to PoS, but the degree of Algorand decentralization is better than the current PoS mechanism in that: 1. the token holdings only affect the probability of being selected as a committee or block proposer, but do not determine the power of generating new block; 2. the consensus process will draw several proposers. The final confirmation block is selected based on Proof of VRF, which guarantees the fairness and unpredictability of leader; 3. Node participation does not require any permission, and anyone who owns equipment can participate in accounting as a node.

After testing practice, Kaleido decentralization degree based on Algorand is higher than any DPoS public chain and most PoS public chains.

2. Extremely High Security

If a system can verifiably resist Byzantine node attack, double spend attack, witch attack, denial of service attack, then we can assure that the security of the system is high enough.

In Kaleido network, the Pure PoS of consensus process does not determine the probability of lottery by the value of the user's token, but selects the winning user according to the balance of each account, which can effectively avoid attackers forging multiple identities and increase the probability of being selected, thus launching witch attacks; secondly, VRF encryption lottery algorithm keeps all users' identity involved in the consensus in secret. Even though the identity is exposed after voting broadcasting and the opponents can corrode them immediately, the messages they send cannot be withdrawn, and the one-time temporary secret key used for signature will be discarded immediately after message generation, which makes the opponent unable to generate any legitimate messages again in this round, greatly enhancing the randomness and unpredictability; furthermore, a block notarization requires randomly selecting members of committees for multiple rounds until consensus is reached, and replacing members of

committees for each round, which can randomly distribute rights to all nodes in the whole network and greatly reduces the possibility of attackers committing crimes and controlling the whole network.

In Kaleido's network, as long as the honest nodes in the whole network have token weights greater than 2/3, the main chain can avoid the possibility of bifurcation and double spending.

3. Low Energy Consumption, Low Bifurcation and High Performance

The consensus mechanism used by Kaleido makes it possible that no matter how many users there are in the system, only one out of every 1500 users will be selected by the system to perform computations for several seconds, which does not occupy computing resources. Ordinary personal computers can also participate in the production block.

Every time only one block with the highest priority is notarized, which means that there will be almost no bifurcation. The

generation of blocks means the finality of transaction information. The Kaleido Consensus protocol completes block validation every few seconds, causing very low latency.

Kaleido's consensus process is based on an ultra-fast Byzantine Agreement (BA*). The speed of encrypting random lots and the notarization of small-scale committee members will bring high throughput to Kaleido on the basis of ensuring network security. At present, the Kaleido test network's output rate is 2 seconds per block, TPS reaches about 3000, and is expected to reach about 5000 after the main line, which is enough to support the application needs of the game market.

4. High Privacy Protection

Despite the anonymity of the transaction subjects in Bitcoin and ETH, the data of transaction amount, transaction time, transaction address and so on are open in the network. Any attacker can trace and analyze these records so as to have a great chance to crack the identity of the transaction subjects。Game bears a high privacy requirement of the data such as transaction

amount. In terms of data storage security and privacy protection, Kaleido implements two kinds of public encrypted accounts by applying ZKPs and homomorphic encryption technology to smart contracts. One is the encrypted token contract corresponding to ERC-20 token, and the other is the encrypted settlement account based on game application which hides the identity and amount of the transaction, and ensures the high security and privacy protection of user accounts.

5. Low-threshold Development and Large-scale Landing

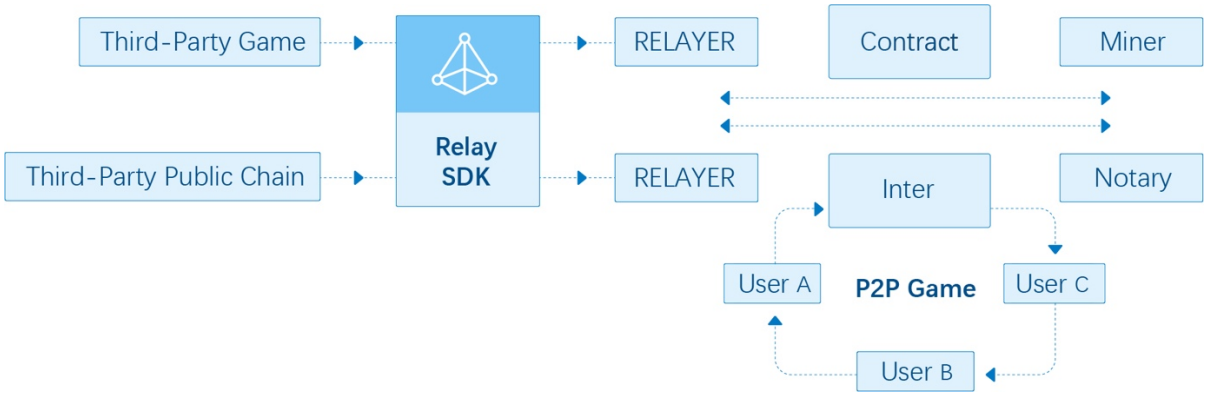
The ultimate goal of all the design of Kaleido public chain is landing of large-scale commercial applications. Therefore, a series of technical explorations and preliminary results have been achieved in three principles: improving the performance and security of the chain, reducing the difficulty of developing and deploying applications, and lowering the threshold of participation of ordinary users. First, the underlying consensus algorithm lays a solid foundation for achieving high throughput and high security; secondly, for developers, we provide a more complete development environment than the existing public

chain, all developers with basic programming knowledge can deploy more personalized and diverse applications on the chain; for general users without any blockchain foundation, participation in the use of applications on Kaleido does not require downloading wallets, gas fees, etc. Experience is not much different from the current App, learning threshold is almost zero, which allows users to enjoy a fair and transparent distributed application and to truly own game assets.

The above makes it possible to apply a blockchain technology to the ground with tens of millions of users.

2 Kaleido Technical Solutions

2.1 Kaleido Overall Collaboration Architecture



2.1 Kaleido Overall Collaboration Architecture

Roles on chain:

- Relayer, as an independent functional unit, acts as an authorization and verification function when accessing third-party public chains (such as BTC and USDT) and is responsible for assisting the main chain in aligning third-party values with contracts in the main chain.
- Contracts, including token contracts and game contracts, etc. Third-party chains can create token contracts and create game contracts on this basis.
- Miners, responsible for achieving consensus process based on Algorand, block validation, packaging and other work on the main chain.
- Notary, as an independent functional unit, can submit signature message data to notarize the message, drive the game contract through notarization, and obtain notarization script from the chain to process the user's notarization request.
- Message Forwarders, which exists as an independent functional unit, is responsible for the message transmission of P2P game network, random selection of game message relay by intelligent routing, and verification according to users' signature.

2.2 Kaleido Basic Tech Units

2.2 Kaleido Basic Tech Units

- Side Chain: responsible for the establishment of P2P network under the chain, the transmission of messages, providing the environment for execution of game scripts, the API interface of P2P network and Game SDK and corresponding functions for the transponders and notaries
- Main Chain: Based on Algorand consensus algorithm, provides block data storage, access interface of system contract on the chain, access interface of contract layer, including access control of contract on the chain, etc.
- Contract Layer: Provides the execution environment of the contract on the chain, reading and writing function of the game script, the interaction between the contract and the P2P network under the chain.

3 Algorand Consensus Mechanism

Since the birth of Bitcoin, the scalability/extensibility of block chains, or the performance of block chains, has always been the bottleneck restricting the wide-spread application of block chains technology. All parties in industry, University and research have done a lot of research and exploration on consensus mechanisms, protocols and algorithms of public chain, but there is still no good solution to solve the "Blockchain Trilemma".

PoW mechanism requires high energy consumption and low performance; PoS mechanism sacrifices a certain degree of decentralization; Hash diagram and DAG solves the consistency rather than accuracy; PBFT is too centralized. These consensus mechanisms strengthen two of the three factors from the triangle, remaining difficult to get the optimal solution from the overall situation.

In Kaleido, we adopt a new consensus mechanism, Algorand. It was first proposed by Silvio Macali, a Turing Award winner and computer professor at MIT. It is a fast Byzantine agreement

protocol with leader election based on random lottery elections, improved based on Pure Proof of Stake and practical Byzantine, which not only solves the problem of Byzantine algorithm centralization, but also supports the real Internet environment. It can reach a consensus safely and efficiently in the asynchronous and untrustworthy network environment, thus truly realizing a pure distributed consensus network.

In addition, we use Super-Fast and Partition Resilient Byzantine Agreement `Algor and Agreement'to replace the original Proof of Work (PoW) consensus algorithm `ethash'. In addition, we independently construct a block consensus acceleration network, greatly improving overall performance of the chain.

3.1 Strengths of Algorand

After practical testing, Algorand consensus mechanism has the following strengths:

Algorand is the best solution to the "Blockchain Trilemma" in the existing consensus mechanism. While guaranteeing decentralization and security, Algorand gives the whole network a

powerful scalability, which greatly expands the application scope of blockchain. dApp developers can focus on the development and deployment of application on the chain and better Improve the use experience.

As for the degree of decentralization, Algorand randomizes the elections of the proposer, the voter and verifier of the election committee by VRF (Verifiable Random Function). It uses the linear superposition of binomial distribution to ensure fairness. This design enables any networked device, including small nodes and retail users, to participate in consensus account keeping. Each round of blocks is elected by a new independent committee, that is, each round of block proposers, voters and verifiers are drawn with VRF encryption, which increases randomness and unpredictability. Under the fault-tolerant property of any partition, even if malicious nodes manipulate the network, partition it and maintain it for any long time, the protocol can still ensure security, that is, the consensus results of all honest nodes are still consistent, and the consensus results will not be affected by malicious nodes.

In terms of security, the design of committee alternation ensures the security of the system to a certain extent; in addition, all users participating in consensus voting know their identity secretly, even if the broadcast reveals their identity after voting, the message cannot be withdrawn and the temporary secret key is discarded immediately, so the attacker cannot corrode anymore; Pure PoS mechanism does not measure the weight of lotter by token value but by account balance, which can effectively avoid witch attacks. As long as the total weight of honest users exceeds 2/3, it can avoid double spending and bifurcation. This algorithm has the characteristics of fault tolerance in arbitrary partitions. Even if the network is manipulated by malicious nodes, partitioned and maintained for any length of time, the consensus protocol can be quickly restored after partition recovery, which makes the attack cost extremely high. Whether attacked at user level, protocol level or network level, it can be safely defended.

Algorand has very high scalability. The VRF-based lottery procedure consumes very little power and runs locally. Nodes do not need to communicate with each other. Normally, it only needs two steps to reach consensus. The zero-branch transaction

confirmation mechanism proven by mathematics ensures that once the transaction is blocked, it can be quickly and credibly confirmed, greatly shortening the transaction confirmation time and eliminating the possibility of chain bifurcation. Without optimization such as fragmentation, the target TPS can reach 5000. This throughput is enough to meet the needs of most current applications, and can be extended to billion users safely and steadily while maintaining high performance.

Algorand is specially designed for pure distributed networks, which is very suitable for commercial applications. It greatly reduces the participation threshold of consensus users. As long as they hold token, they can participate in the chain's production process and the community co-governance.

3.2 Execution of Algorand

Algorand runs an improved high-speed Byzantine voting protocol (BA*) based on gossip network. Similar to the preparation, preparation and submission of PBFT, Algorand also has three voting processes of "initiating proposals", "pre-voting" and "confirmation". In addition, the "next round" of voting has been

added. Compared with PBFT, Algorand's improvements mainly include the following points: 1. running on clock frequency instead of time points, which solves the problem of time synchronization in open networks; 2. allowing the first two steps of voting to be executed in parallel, shortening the time required for voting, so that only two steps of voting time is needed to reach consensus under normal circumstances; 3. under abnormal circumstances, the added "next round" voting can make the effective information of the current round of voting pass to the next round, and improve the probability of consensus in the next round. If the probability of multi-round voting is accumulated, the probability of consensus can be greatly improved.

(1) Basic Concepts

Node

We call a client process running on a user device a node. There are three types of nodes on the Kaleido network:

- Mining Node: Implementing consensus block process, which is divided into two roles: sponsor and member of voting committee. Specific functions will be described in detail

below.

- Non-Mining Full Node: It does not perform mining, provides accelerated or business access services, and synchronizes all data nodes in the chain, usually servers or PCs.
- Light Node: Mainly the various clients or wallets of the game in the chain, they do not save blocks and transactions, and access the network by connecting the whole node.

Mining Nodes/Miners

Mining nodes, referred to as miners, are nodes that run consensus algorithms. They run on gossip networks and generate new blocks for the chain. According to the specific functions, it can be divided into:

- Proposer: Responsible for giving block proposals, replace in each round of lottery, up to 26 maximum probability in Kaleido network.

- Committee Member: Work in a group collaborative manner, verify the validity of the blocks given by the proposed miners, vote on the consensus blocks according to the algorithm

logic, and replace through drawing lots in each round.

It should be noted that each mining node randomly draws lots to determine whether it can participate in a round of consensus with a certain role based on the voting weights held. Mining nodes can only increase the probability of winning the lottery by increasing the voting weights held, but cannot affect which role they become.

Keys，Users and Owners

In general, the public key is equivalent to the user, the owner usually means to have the right to use the wallet, that is, to own the private key corresponding to the public key. When one public key j is paid to another public key i, it can be understood that user i joins the system.

Permissionless and Permissioned Systems

If a public key can join the system at will, and a user can have more than one public key, then this is a system without access, otherwise it is a system that needs access.

(2) Assumed Requirements

In order for the system to run normally, it needs some assumptions:

- The system works well in an environment whether access is required or not, and performs better in an environment where access is required.
- There are honest users and malicious users in the system, honest users abide by predetermined rules and behavior guidelines (mainly referring to Byzantine agreements), and can send and receive information perfectly. Malicious users violate any predetermined rules, namely Byzantine errors.
- More than two-thirds of the amount of money belongs to honest users in an environment without access, and more than two-thirds are honest users in an environment where access and “one person one vote” is required.

(3) Target

Ideally, the ultimate goal of the Algorand Consensus Agreement is:

1. Consistency, that is, all honest nodes get the same results and conform to the consensus agreement;
2. Liveness, that is, all honest nodes involved in consensus, can finally reach a consensus result, that is, either reaching consensus or not.

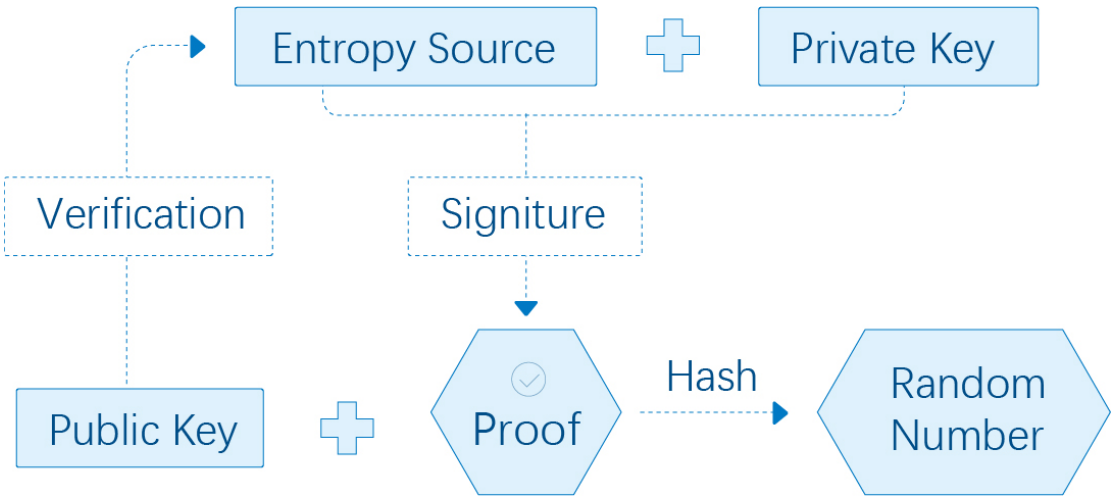
(4) Block Generating Process

Verifiable Random Function

Algorand maintains a very safe and reliable random number VRF, randomness is provided by a hash algorithm with random characteristics, and security is guaranteed by the mechanism on the chain, that is, the public key of mining nodes requiring the update of random numbers is written into the block chain before updating.

VRF provides a random data generation method. The output of the function consists of random results and random proofs. Because it contains the private key signature of the generator, the verifier can confirm the validity of the random number through the public key.

When a user enters a seed + private key, he will get a unique random output and proof. The simple schematic diagram is as follows:



3.1 VRF Generation Process

Algorand Two-step Consensus

1. the proposal of a candidate block; 2, to reach a consensus by BA* algorithm

Algorand is a pure PoS consensus algorithm. Each node participating in the consensus has a weight, which is proportional to the balance of the account. Each node uses the random number in the previous block as seed, carries out the random

lottery algorithm by itself and knows whether it will participate in a specific step of the voting protocol. The lottery result will generate the lottery certificate, which can be checked by any node. When voting, you need to bring your own visa and signature to show your voting rights. This mechanism ensures that the number of nodes participating in consensus in each round does not increase with the increase of block chain distributed network, so that consensus protocols can always run efficiently.

From the above consensus process, we can conclude that Algorand consensus mechanism has the following characteristics:

1. The possibility of bifurcation is very low.
2. The amount of calculation needed is very small.
3. The delay of generating a block on the chain is similar to the delay of completing block broadcasting in the network.
4. Network nodes are not required to be on-line 7*24 hours (Lazy Honesty).

3.3 Token Circulation Model

The characteristics of Kaleido consensus algorithm determine that a large number of miners are needed to ensure the stability

and safety of the underlying system. Therefore, the design of Kaleido must embody the economic incentives for miners to benefit from their efforts, so as to promote the benign development of the underlying ecosystem. In addition, the ecological prosperity of the Kaleido public chain is crucial. All participants who make positive contributions to the ecosystem, including game developers, players and strategic partners, should be awarded to match their contributions.

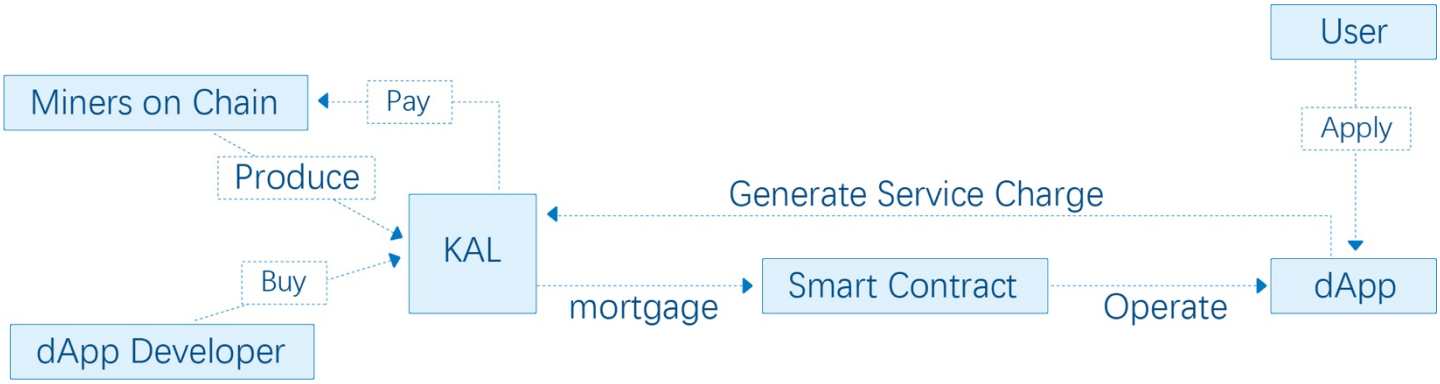
Therefore, the design of Kaleido token flow model should follow these principles:

1. On the basis of guaranteeing the safety of the bottom chain, we should attract as many high-quality miners as possible into the bottom ecosystem to participate in consensus building. A large enough number of miners can guarantee the realization of the condition that 2/3 of the miners are honest nodes and satisfy the major premise of stable and safe operation of the system.
2. Let all the miners who contribute to the safety and performance of the chain obtain the corresponding remuneration according to

their own labor, which is predictable, auditable, traceable, fair and impartial, and cannot be tampered with.

3. As the bottom platform of application development, token's mobility, including output, use and consumption, is very important to promote the sound operation of the whole ecosystem. As a fuel agent, token should guide ecological participants to use and consume, rather than hoard and hype.

Based on the above principles, Kaleido token's circulation economic model is as follows:



3.2 KAL Token Circulation

(KAL is short for Kaleido token)

4 Trustworthy P2P Network

4.1 P2P Network Communication Mechanism

Transaction throughput and delay are the most important performance indicators. The transaction performance of block chains is affected by broadcast communication, information encryption and decryption, consensus mechanism and transaction verification mechanism. As one of the core technologies of blockchain, the efficiency of P2P network communication has a great impact on performance.

The traditional P2P network applies anonymous message interconnection based on tracker or DHT mechanism, which adds randomness to the network. Because of the untrustworthiness between nodes, hash is not only used for checking important data in messages, but also requesting and retrieving when communicating requests data. However, there is no checking for the sender of messages, which is not suitable for application in game logic, because applications and games usually drive state-changes based on participants' messages.

The P2P network we implemented adopts Notify-based broadcast mechanism. All nodes in the P2P network will receive all messages with their signatures. Therefore, each user can verify the messages in the network. At the same time, the users in the P2P network can authenticate according to the status of the chain, so as to ensure the credibility of P2P network established downlink. In addition, Notify mechanism ensures that each node is completely equal, so that a single node can verify all application logic.

5 Game Script Driving Framework Based on Trustworthy P2P Network and Smart Contract

Kaleido can build more complex decentralized applications by combining trusted P2P networks with on-line contracts. Chain book is the data and status switching mechanism of each application, while the interaction of P2P network is the extension under the chain, responsible for completing the game logic and reaching the consensus under the chain. In a trusted P2P network,

through zero-knowledge proof of cryptography and signature of trusted data, it can be extended to more trusted data interactions completed through centralized servers.

6 Open Encrypted Account

One big challenge of blockchain open account applied in the game industry is privacy. Whether it's Ethernet or Bitcoin, the transactions and account balances on the chain are open to everyone, while the game industry requires high data privacy and is very sensitive to the game transaction data. Therefore, we design an encryption account implementation mechanism with a higher level of privacy for the game industry.

6.1 Homomorphic Encryption

Homomorphic encryption is an encryption algorithm that can directly calculate the encrypted cipher text to get the original data cipher text. Homomorphic encryption algorithm can delegate computing to a third party without revealing the original information, so that cloud computing based on privacy data can be realized. Homomorphic encryption algorithms that can

implement all algorithms (addition and multiplication) are called homomorphisms. Encryption algorithms with homomorphic properties are proposed by IBM, but homomorphic algorithms cannot be applied to real business scenarios for now due to the limitations of current computing power. For an encrypted account, only a homomorphic encryption algorithm with homomorphic addition characteristics can realize the encryption and operation of the account.

We choose an encryption algorithm with homomorphic addition to encrypt the account, and implement the encryption operation in the API under the chain. Only data operation (i.e. transfer) and verification are carried out in the account (i.e. contract), so that realizing an encrypted account which can be applied in the real scene.

6.2 Zero Knowledge Proof

A highly public and fair encrypted account book cannot be achieved only through an additive-based homomorphic encryption algorithm because the data of public account book need to be submitted by multiple parties and it is difficult to

ensure that the data submitted is valid and not intentionally cheating. Thus, it is much more difficult to realize a public encryption account book that anyone can participate with correct data.

We use zero-knowledge proof to ensure the validity and correctness of data submitted by participants. In the actual transfer process, participants are required to submit proof of data validity and correctness, and encrypted data in the transfer transaction can be verified by using zero-knowledge proof.

7 Privilege Control Contract Mechanism Based on Smart Contract

One of the barriers to large-scale promotion of blockchain dApp to the general public is that users must hold the designated token on chain, and the main way to get cryptocurrency is on the exchange. At present, the users of blockchain application are basically those who hold the token of various projects, coupled with the poor experience of dApps, it is difficult to expand the number and scale. However, if blockchain as a revolutionary

technological innovation should ultimately realize large-scale landing, users must be able to easily participate in the application experience and enjoy the technology dividend without any technical knowledge or financial threshold, so as to truly reflect the value of blockchain.

Therefore, applications deployed on Kaleido must be directly used without needs for users to know the expertise nor transactions through exchanges, just like today's Internet applications.

The gas mechanism on Ethereum effectively protects the security, and effectively controls the attack of DDoS by requesting the caller to pay the gas. But at the same time, because the miners choose transactions according to the price, it leads to blockading the normal transaction by sending high-price transactions. Therefore, we have implemented a mechanism that can control the type of transaction and verify validity and authority of the transaction.

8 Kaleido Application Scenario

Without sharding parallelism, Kaleido's TPS targets at around 5000, which is enough to handle most of small and medium-sized commercial applications, but still insufficient in dealing with large-scale game dApps. We plan to add layer 2 sharding parallel computing framework in the second half of 2019 to further upgrade TPS to about 30,000. We believe that this magnitude is enough to support 99% of commercial applications up to now. Algorand consensus mechanism has no restrictions on the number of user access, and open user access mechanism of Kaleido P2P network is sufficient to support large-scale user use.

As a public-chain platform that focuses on games and supports more distributed applications, Kaleido's first landing application scenario aims at the global game market. Judging from the trend of last Internet technology wave, the earliest explosive growth point of information internet is game. In the era of value internet, we believe that game is also one of the explosive points of killer applications.

To verify the feasibility of Kaleido's landing, the founding team has developed a game demo called Fight Against Landlord, the most popular Chinese game, based on Kaleido, which will be the first Fight Against Landlord based on the pure distributed blockchain network in the world. Demo tests show that the experience and interaction are the same as running on centralized servers. At the same time, the whole game process is chained from betting, licensing to final settlement. There is no unilateral control of results, and it can be retrospectively audited afterwards, so that the game results cannot be tampered with. In addition, the rules can be made public based on Algorand consensus mechanism, which ensures the transparency and fairness of game process, and guarantees the game assets ownership of players.

9 2019 Annual Development Plan

- February: continuous optimization of test net and game demo; game ecological construction; first batch of partners docking
- March: Kaleido application developer tools on line: test net, game demo test edition, developer document; game

community building; partner docking

- April: Kaleido main network officially launched; miner incentive plan finalized and launched; game officially demo online; third-party developers' participation
- May: official online game version on line; large-scale game player promotion kicks off; SDK development documents on line; encrypted book on line
- June: third party game release and operation; BDN on line test net; complete third party development document publication
- July: holding large-scale online competitions; docking strategic cooperation in the industry
- August-September: complete layer 2 scheme on line; sharding scheme verification; BDN formal scheme on line
- October-December: release of sharing solution and storage solution; Virtual Machine Optimization

10 Conclusion

After preliminary research and development and practical testing, we designed and demonstrated the landing feasibility of a next generation high-performance blockchain game platform.

Algorand, an improved consensus mechanism based on VRF and PBFT, is the basis of decentralization, security and performance. On this basis, we construct a trustworthy P2P network, a game script-driven framework based on P2P network and smart contract, two open encrypted accounts and a privilege control contract mechanism. In the landing application scenario, we will plough the game market in the early stage, and design a sound token economy model for the technology layer, middle layer and ecological layer to promote the operation of gears through token fuel.

Next, Kaleido will continue to upgrade and optimize the underlying infrastructure, and focus on construction of the ecosystem to achieve closed-loop circulation of ecological value. In game industry which is a high-value market, we believe that the game based on blockchain P2P distributed network will go further than bringing more fair, transparent and pure game experiences to players. The revolutionary significance lies in establishing a stronger trust link for all ecological participants, so that game developers, operators and players can fully meet their needs. Therefore, a strong consensus is formed on the basis of common

interests, so as to endow the whole game ecosystem with vitality and prospects.

In the future, Kaleido public chain will expand from the game to more fields, aiming at Linux system of blockchain.

References

[1] S, Nakamoto. Bitcoin: *A Peer-to-Peer electronic cash system*. http://www.bitcoin.org/bitcoin.pdf, May 2009.

[2] *Bitcoin Computation Waste*, http://gizmodo.com/the-worlds-most-powerful-computer-network-is-being-was-502013.

[3] BitcoinWiki. *Proof of Stake*. http://www.blockchaintechnologies.com/blockchain-applications.

[4] Ethereum Foundation. *Ethereum,2016*: https://www.ethereum.org.

[5] Jing Chen, Silvio Micali. *ALGORAND*. In arXiv report http://arxiv.org/abs/1607.01341 Version 9.

[6] Yossi Gilad, Rotem Hemo Silvio Micali, Georgios Vlachos, Nickolai Zeldovich. Algorand: *Scaling Byzantine Agreements for Cryptocurrencies*. In SOSP '17.

[7] Silvio Micali, *Byzantine Agreement, Made Trivial*. http://people.csail.mit.edu/silvio/SelectedScientif

[8] B. Chor, S. Goldwasser, S. Micali, and B. Awerbuch. *Verifiable Secret Sharing and Achieving Simultaneity in the Presence of Faults*. In Proceeding 26th Annual Symposium on the Foundations of Computer Science, IEEE,1985:383~395

[9] Silvio Micali, Salil Vadhan, and Michael Rabin. *Varifiable Random Functions*. In FOCS'99.

[10] S. Goldwasser, S. Micali, and R. Rivest. *A Digital Signature Scheme Secure Against Adaptive Chosen-Message Attack.* SIAM Journal of Computing, 17, No. 2, April 1988, pp. 281-308
[11] S. Micali. *Fast And Furious Byzantine Agreement.* Innovation in Theoretical Computer Science 2017. Berkeley, CA, January 2017. Single-page abstract.
[12] B. Chor and C. Dwork. *Randomization in Byzantine agreement, in Randomness and Computation.* S. Micali, ed., JAI Press, Greenwich, CT, 1989, pp. 433-498.
[13] D. Dolev and H.R. Strong. *Authenticated algorithms for Byzantine agreement*. SIAM Journal on Computing 12 (4), 656-666.
[14] M. Castro and B. Liskov. *Practical Byzantine Fault Tolerance, Proceedings of the Third Symposium on Operating Systems Design and Implementation*. New Orleans, Louisiana, USA, 1999, pp. 173–186.
[15] M. Pease, R. Shostak, and L. Lamport. *Reaching agreement in the presence of faults.* J. Assoc. Comput. Mach., 27 (1980), pp. 228-234.

Drop a Line：info@kaleidochain.io