Aurora

Technology White Paper

Version2.0

Aurora Foundation

August,2019

Table of Contents

Preface

1.1 Background

In 2008, a pseudonym of Nakamoto Satoshi submitted the groundbreaking paper "Bitcoin: A Peer-to-Peer Electronic Cash System" to the Metzdown Cryptography mailing list, before then publishing the initial implementation code in 2009. The first bitcoin was generated on January 3rd 2009 at 18:15:05 (UTC). The Bitcoin model was unprecedented in that it solved the problem of double-spending on digital ledgers. The next two years witnessed rapid growth of both public and developer interest. It is a project that began with speculation and experimentation, but which has inspired a broad movement that will change the world.

Subsequently, a series of payment-related digital currencies such as LTC, DOG, XRP, and PPC have emerged. The development of blockchain technology in this early period focused primarily on digital currency and applications offering currency transfer services, exchange, and payment. Along with Bitcoin, these services represent Blockchain 1.0, which was largely focused on decentralized money and payments.

The vision statement that Nakamoto laid out in 2010 had three core components: Decentralized publicly traded ledgers, end-to-end direct value transfer systems, and powerful scripting systems to run any agreement or currency.

Bitcoin achieved the first two goals, and the third was implemented with Ethereum, which released a white paper in 2014 and officially launched in 2015. Ethereum is an open-source, infrastructural decentralized system upon which blockchains and protocols can be run. It builds a common, low-level protocol that both provides a Turing-complete scripting language and executes smart contracts on the system. By deploying and running smart contracts, Ethereum demonstrates that blockchain can be used to facilitate transactions and build networks in highly complex scenarios. Ethereum released the application power of blockchain technology, and is considered to be Blockchain 2.0.

In the Blockchain 2.0 era, blockchain provides a trusted run-time environment for smart contracts, which are the foundation of blockchain applications. The applications of this technology extend far beyond payments. Many companies and governments are now exploring new application cases built on smart contracts.

Blockchain-based smart contracts and applications are still in their infancy; real adoption driven by truly useful applications has yet to happen. This said, however, the vast,

transformative potential of these technologies is clear. Open source, decentralized applications are the way forward, and the inevitable development of novel and impactful applications will profoundly shape modern society.

1.2 Third-Generation Blockchain

We believe that third-generation blockchain technology will extend Blockchain 1.0 and 2.0 frameworks to revolutionize the entire technology industry. A complete blockchain ecology cannot be isolated, it should be interconnected, synergistic, and large-scale. Most of all, an ecology should be flexible enough so as to evolve in step with changing needs and technological innovation.

Third-generation blockchain technology can both drive the real economy and serve as the core of the value internet. Fully functional Blockchain 3.0 will allow tokenized tangible and intangible assets to be measured, tracked, controlled, and traded on chain. By constructing a safe, environmentally friendly, efficient, intelligent, and scalable technology ecosystem, Blockchain 3.0 will realize the mapping and transfer of various asset rights in the parallel time-space of the real and digital worlds.

When blockchain can be meaningfully applied to the field of social governance, in other words to the domains of science, culture, art, health, games, e-commerce, etc., we can say that it is entering the Blockchain 3.0 era. The range of blockchain applications is limitless, and early stage applications currently address: digital identity authentication, notarization, arbitration, auditing, domain name, logistics, medical, mail, travel permits/visas, voting, and more. Indeed, Blockchain 3.0 will likely become the foundation of the "Internet of Everything."

1.3 Opportunities

Applications built on advanced technology will determine the future.

Blockchain technology has moved from an initial phase of speculation and research to application development.

Retail

Retail is one among a range of industries where blockchain technologies can have a meaningful if not revolutionary impact. The retail industry continues to develop globally, particularly online. However, centralized operations bring many drawbacks. Traditional e-commerce products usually go through sales, marketing, logistics, warehousing, and

distribution before reaching the consumer. The entire supply chain process is undisclosed. Further, distribution is expensive, and customers are unable to determine the origin and authenticity of their goods. These problems are particularly acute in the food, medicine, and luxury sectors.

Aurora is building a set of core, decentralized solutions to address these pressing problems. By integrating decentralized trading systems and integrated blockchain payment systems in a logistics application framework, Aurora will offer end-to-end tracking and payment services for retail providers and customers.

Gaming

Online gaming is increasingly popular and today's consumers spend far more time and money on games than in the past. Games have evolved in such a way as to create massive online communities of fans and gamers who actively exchange content as well as virtual prizes and items obtained in a game itself. The traditional game industry is mainly composed of game developers, game operators, game channel providers, payment service providers and game players. Game operators use their own resources to coordinate various offerings and provide services such as operations, promotion, and revenue settlement after a product goes online. Operators who gain in popularity earn proportional voice and influence in the industry chain, and frequently expand development through acquisitions and other means. This model significantly raises the barrier to entry in the traditional game industry sector. In such contexts, the game mechanisms become opaque, independent developers are excluded, and game content is fixed. Blockchain solutions redefine the relationship between game developers, game makers, and players, offering developers and players active roles.

At present, a few entrepreneurs have developed blockchain games that are popular among players. Although the blockchain game industry has developed rapidly, the volume is still small, the in-game mechanism is relatively simple, and the development space is large, and even internet giants such as Google, Microsoft, Baidu, NetEase, and Tencent have begun to gradually explore blockchain game business to capture more market share. Aurora's game industry applications can help DAPP developers quickly bring their products to market. Even more, Aurora decentralized solutions will address fraud, asset distribution, fairness, and data black box operation.

Finance

Financial institutions require a credit mechanism that can be built on the Internet. Blockchain can potentially impact virtually every branch of finance, leading to a beneficial and systematic restructuring of the entire industry.

In the field of payments, the cost of reconciliation, clearing, and settlement between financial institutions, especially cross-border financial institutions is very high, and entails a large number of manual processes, making the micropayment business difficult to carry out. In the securities field, data securitization faces three major problems: it is difficult to access, difficult to analyze, and difficult to update in real time. In the field of auditing, audit data is difficult to obtain, audit work is difficult to carry out, and overall, the process relies heavily on manpower. In the field of user identification, efficient interaction of user data between different financial institutions is difficult to achieve, which results in high costs of repeated authentication and indirectly, to the risk of user identity being leaked by intermediary agencies. In the field of asset management, assets such as equity, bonds, notes, and income certificates are hosted by different intermediaries, which increases the transaction costs of such assets and brings problems such as the possibility that the documents may be forged.

The public blockchain built by the Aurora project – the Aurora Chain -- is data tamper-proof and traceable, enabling point-to-point value transfer. Both parties can bypass third-party direct transactions, realize quasi-real-time asset transfer, and speed up transaction clearing. Through the digitization of assets and the reconstruction of the financial infrastructure, the efficiency of the financial assets after the transaction, the settlement process, and cost reductions can be greatly improved.

1.4 Aurora and its Vision

Aurora is a decentralized application platform based on third-generation blockchain technology, dedicated to providing mature blockchain technology solutions for multiple enterprise needs.

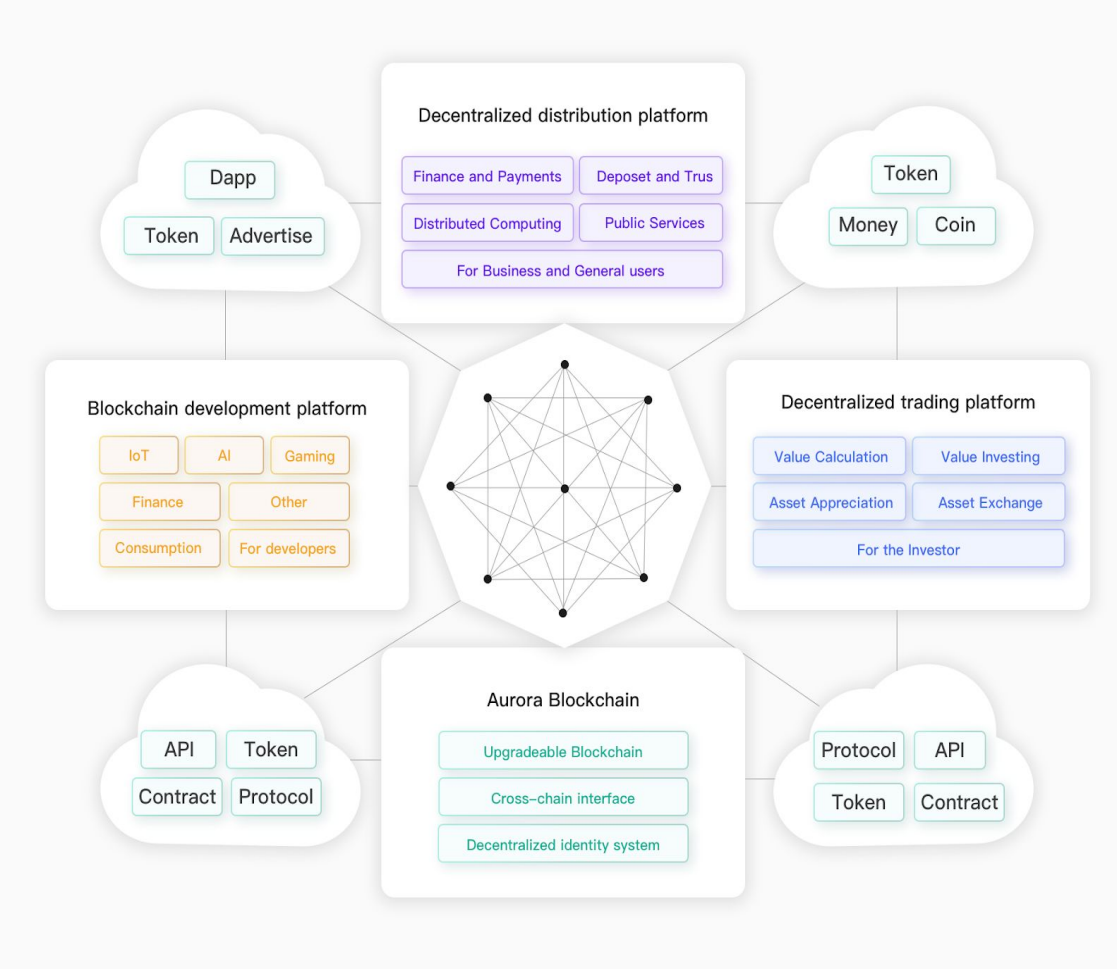
Aurora's goal is to integrate blockchain into different industries such as finance, e-commerce, games, and the Internet of Things. The entire Aurora infrastructure deploys scalable technology to support multi-chain operation, and to bridge between blockchain technology and industries including gaming, finance, e-commerce, and beyond.

Aurora is building vital enterprise solutions that are sustainable and built for current and future needs. The Aurora mission is to provide a complete, blockchain-based industrial ecosystem that will increase operational efficiency and promote resource sharing.

2. Ecological Architecture and Use Cases

The Aurora public chain and the Aurora chain platform together form the backbone of the Aurora ecosystem. In a decentralized framework, the platform supports application

integration R&D, an application distribution system, a game/DAPP exchange, a universal identity system, and a payment service. Applications and platforms have been designed to be both user and developer friendly.



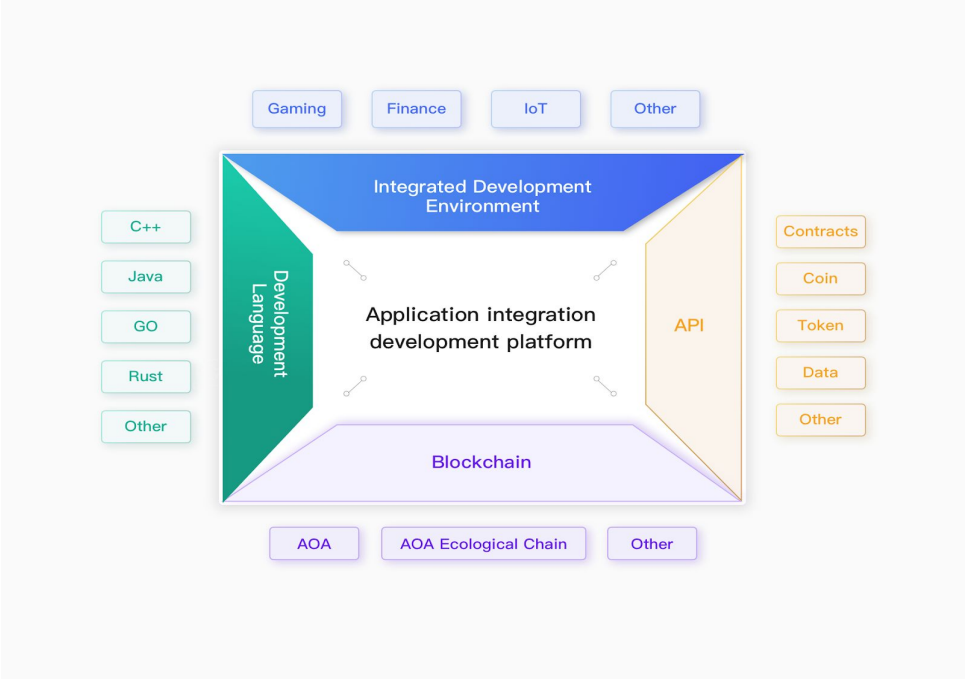
2.1 Aurora Chain

Aurora Chain provides commercial-level decentralized services including the Themis consensus mechanism, cross-chain capabilities, and a stable, customizable, and easily upgraded framework. The Aurora Chain supports upgrade iterations without the need for forking. What's more, the system is scalable and under the right conditions, transaction speeds are limitless.

The Aurora Chain will work with developers and industry leaders to empower the real economy with blockchain technology to drive the digital economy and provide users with a variety of decentralized applications to create a new blockchain 3.0 ecosystem.

2.2 AuroraDev

Developers can use the AuroraDev which is Aurora-chain-based application integration platform to rapidly develop blockchain DAPPs and minimize development costs.



The AuroraDev application R&D integration platform can connect the Aurora Chain and various integrated development environment IDEs and API interfaces. It also supports multiple mainstream development languages and SDK software development kits. Developers can quickly customize interfaces based on existing frameworks to meet specific business function requirements.

AuroraDev focuses on the writing, compiling, deploying, interface testing of smart contracts and the deployment of DAPP and third-party applications, all supported by the built-in development frameworks, including debugger and test environment. After a contract is written, it will be automatically compiled according to the type. After compiling, it can be deployed to the sandbox environment, and the call interface corresponding to the contract will be automatically generated.

The Gaming Industry:

In the existing game ecosystem, developers generally contend with long game development times, high costs, a lack of suitable development tools, and insufficient game development and network-side operating environments.With AuroraDev, developers can easily access

frameworks such as open source software development kits (SDKs), smart wallets, game plugins, and payment platforms to quickly develop game DAPPs and publish them to minimize development costs. The development language used by developers around the world to develop games are the LUA and JavaScript scripting languages. Currently, many blockchains only support C++ or Go, a limiting factor for game developers accustomed to working in other languages. AuroraDev's support allows the Aurora Chain to interface with multiple programming languages, allowing game developers to easily transition to blockchain development.

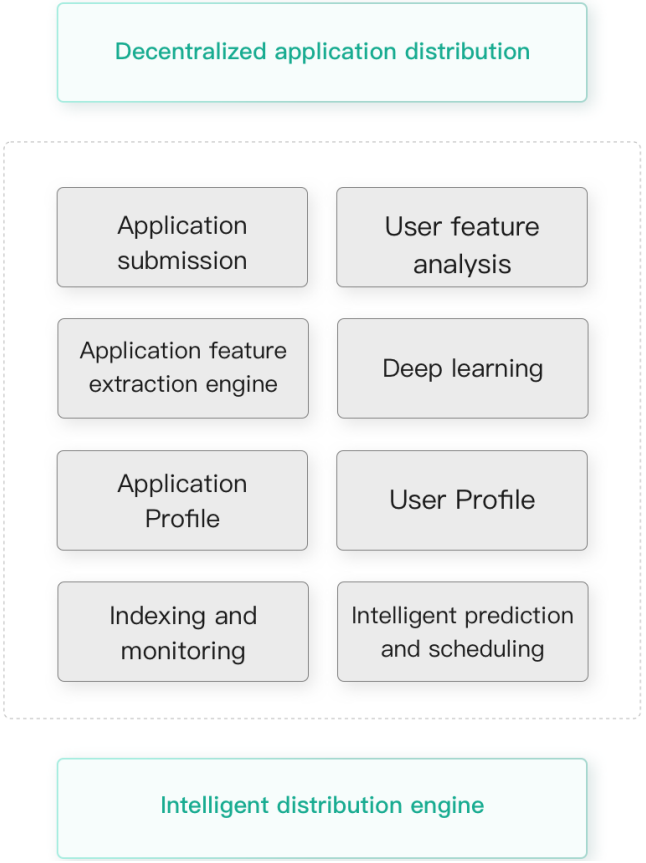
2.3 AuroraDist

Various industries, especially applications and e-commerce, have entered a mature stage in marketing. In the increasingly fierce competition environment, it is imperative for companies to solve the problem of how to break through the limitations of current marketing practices.

In the domain of online operations, marketing success is measured by network traffic. But the real value of this traffic is opaque. But a successful marketing campaign is built on much more than traffic.

Aurora decentralized application distribution system AuroraDist is built by Aurora, developers and players. It has a built-in intelligent distribution engine that can index and monitor through big data, and use the application feature extraction engine to image and classify applications. At the same time, the decentralized application distribution system can create a profile of user behavior and perform deep learning through big data for user feature analysis. Such capacities enable precision marketing. AuroraDist will create a new management and incentive mechanism as well as a multi-level referral system. Users can promote high-quality DAPPs on the platform, allowing users to participate in distribution channels, benefit from corresponding value incentives, and earn extra income.

Take the game industry as an example:



The problem of traditional Internet game distribution is quite serious, such as oligopoly, long payback period, unreasonable distribution of interests, etc. Over-reliance on game publishers has caused developers to be highly squeezed, and customer acquisition costs remain high.

Game developers can use distributed storage to quickly upload distributions to AuroraDist, enjoy the precise user matching brought by the intelligent distribution engine, and easily implement complex policy requirements such as paid downloads. Games on the Aurora Chain can access on-chain data, direct users, and minimize distribution and customer acquisition costs. At the same time, through incentive mechanisms, players can obtain pass-through incentives by promoting high-quality games and thereby become a part of the distribution process. Aurora can also help game operators on the platform to establish an open and transparent competitive incentive and ranking system. This system mainly uses the blockchain to record the duration of the game and the number of upvotes to achieve the game's ranking and ensure authenticity.

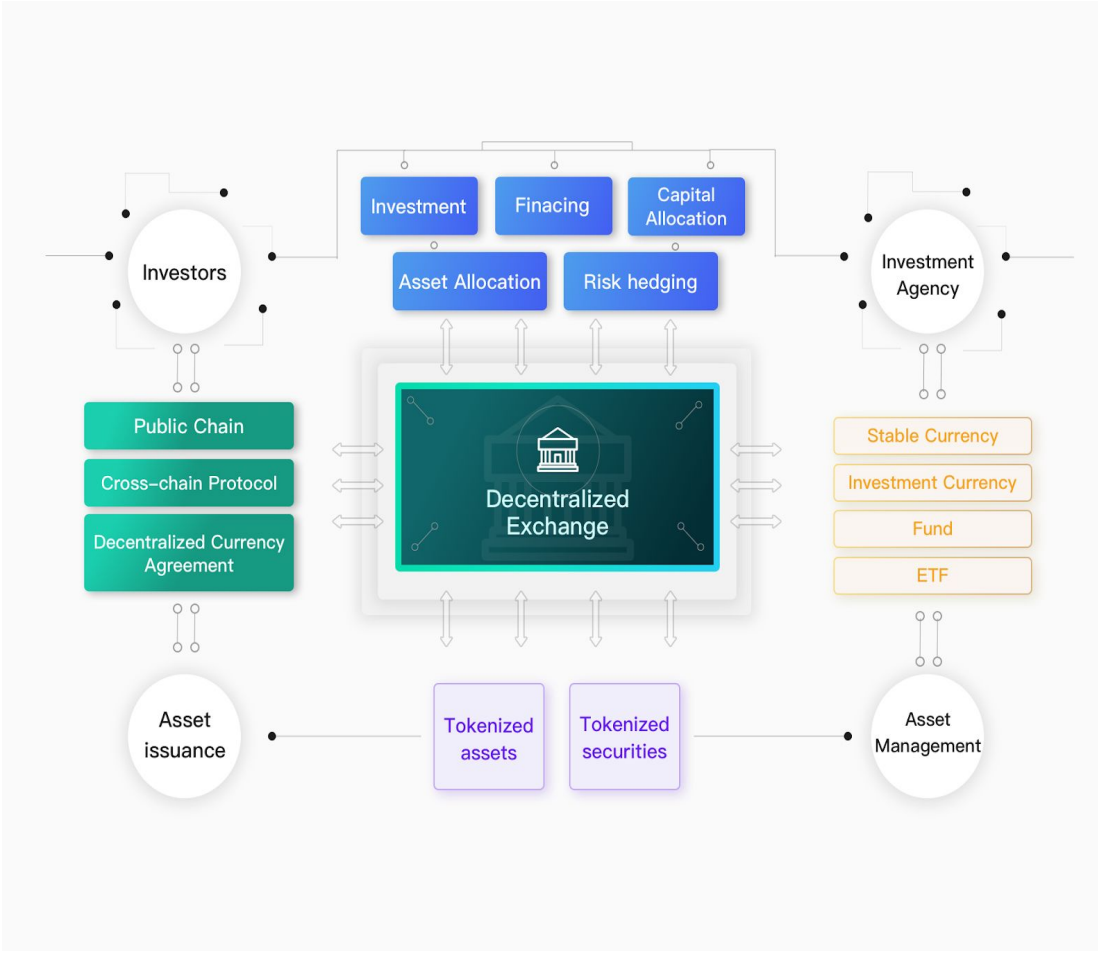
Take the financial industry as an example:

The new market environment and policy changes have brought various marketing challenges to the financial industry. The overreliance on network traffic data, the cost of customer retention, lack of user insight, and inadequate delivery strategies are the pain points of financial industry marketing.

AuroraDist can identify user needs to better help developers address their clientele . The Aurora platform analyzes user profiles (occupation, education-level, and various financial attributes) to offer actionable data that can be used to build targeted marketing plans, improve customer service and drastically reduce marketing distribution costs.

2.4 Decentralized exchange——AuroraDex

Valuable assets need to flow between i)the traditional economy and the crypto-economy, ii)different entities of the crypto-economy, and iii)different blockchains.



For financial assets, various assets, such as equity, bonds, income certificates, warehouse receipts, and bills, can be integrated into Aurora's decentralized trading platform, AuroraDex, to become a digital asset on the chain. Such free trade allows asset owners to initiate transactions directly without having to go through various intermediaries. In AuroraDex, industry infrastructure organizations can act as custodians, ensuring the authenticity and compliance of assets, thereby building a bridge between managed libraries and distributed ledgers, and further enabling distributed ledger platforms to securely access trusted assets in managed libraries . Asset issuance can be carried out in a confidential or public manner as needed.

The trading of financial assets is a contract between the relevant parties based on certain rules. AuroraDex can fully express these business logics with code, such as fixed income securities, repurchase agreements, various swap transactions and syndicated loans, etc. The

automatic execution ensures that the relevant contracts are only visible between the counterparties and are confidential to unrelated third parties.

For in-game assets, standard tokens and virtual objects in the Aurora Chain blockchain ecosystem can be traded directly across the game.

In the game trading, players face various problems, such as the centralization of pending orders, high global game cross-border transaction fees, un-locateable equipment. In response to these problems, the decentralized exchange AuroraDex can facilitate fair trading, including virtual items such as props, equipment, and skins in the game. The AOA token establishes a unified standard of value across the blockchain ecology, allowing cross-platform transactions.

AuroraDex will build a virtual asset database, and players' props, equipment, tokens, and circulation paths will be recorded on the Aurora Chain. This data is transparent and open, allowing players to easily control their assets and track categories and quantities.

With regard to the e-commerce industry, buyers and sellers on AuroraDex set transaction information in advance. Consensus mechanisms and multi-signature of the Aurora Chain mean that buyers and sellers do not need to trust a third party to conduct transactions. Enterprises and merchants maintain their own business model and profit model.

By deploying smart contracts, AuroraDex can perform delayed transactions and automate contracts without any intermediary parties. At the same time, it supports cross-chain interaction, which enables broad networks of exchange.

In addition, AuroraDex can address the reliability pain points in e-commerce trading platforms. In the traditional e-commerce trading platform, there is conventionally only one security agent who is responsible for identifying untrustworthy actors. In the AuroraDex and Aurora Chain trading networks, all participants (merchants and customers) can access transparently available information to help secure the system.

2.5 AuroraDID

Decentralized Universal Identity System - AuroraDID

The digital identity of all users in the Aurora blockchain ecosystem - AuroraDID can be shared among different applications, enhancing the community's sense of belonging and

loyalty. Each user identity information and assets within the account are owned by themselves and do not belong to any third party.

In traditional applications or games, users have to register different accounts when using different applications or playing different games. The more apps and games they play, the more account IDs and passwords they have, and the account management is quite troublesome. Traditional applications and game accounts are forced to attach to the manufacturer's server, not owned by the user, and can never be transferred out of the server. When users are tired of an app/game and want to switch to another, they will face a very awkward situation that they have to abandon all account information. However, in the Aurora ecosystem, AuroraDID can be shared among different DAPPs, avoiding the hassle of registering multiple accounts, and the user's identity information and asset data in the account will not be abandoned, which greatly enhances the sense of belonging and loyalty of the Aurora community.

In addition, in the traditional financial industry, identity verification is indispensable in many business processes. User data between different financial institutions is difficult to achieve efficient interaction. The cost of repeated authentication is high, and indirectly brings the user identity to the risk of an intermediary leaking. In addition, when personal identification documents are lost, especially in cross-border situations, this problem becomes more troublesome. The problems caused by these authentications can be effectively avoided by using AuroraDID for authentication in the Aurora ecosystem. The Aurora Chain can make the transmission of such sensitive information more convenient and efficient. In addition, through the intelligent contract unique to the Aurora Chain, the identity verification system can selectively display personally identifiable information and achieve local sharing of identity information within the relevant scope. Under the premise of information sharing mechanism, it can prevent identity theft while protecting privacy.

At the same time, in the traditional e-commerce transaction payment, the user needs to perform a series of operations such as registering the account, uploading identity authentication, and the transaction process will record the mark on the central organization. If the supervision is missing, a large amount of sensitive information may be leaked. The decentralized identity of the Aurora Chain uses efficient zero-knowledge proof, and privacy protection based on cryptographic schemes such as elliptic curve digital signature and BLS signature to ensure account security.

2.6 AuroraPay

Open Integrated Blockchain Payment System - AuroraPay

AuroraPay, an open-chain integrated blockchain payment system, is a unique open blockchain payment system that supports a variety of assets in the Aurora ecosystem. The DAPP inter-payment system is completely open and is not limited to assets on the Aurora chain.

AuroraPay can achieve lower fees, faster payments, safer transactions, lower payment cost, and increase profit margins for developers. AuroraPay can also speed up the transaction settlement, and promote efficient and affordable payments.

Currently, payment and settlement of most daily applications and games are extremely inconvenient. Operators and channel providers have serious trust problems, especially for multinational operations with complicated and costly payment channels. Aurora chain cross-chain technology fully open DAPP inter-payment system can break through the problems of the centralized mechanism and the monopoly of a single bookmaker. It provides a completely transparent and traceable trading system for users and developers in the ecology, as well as a fair, safe, simple and anonymous payment method.

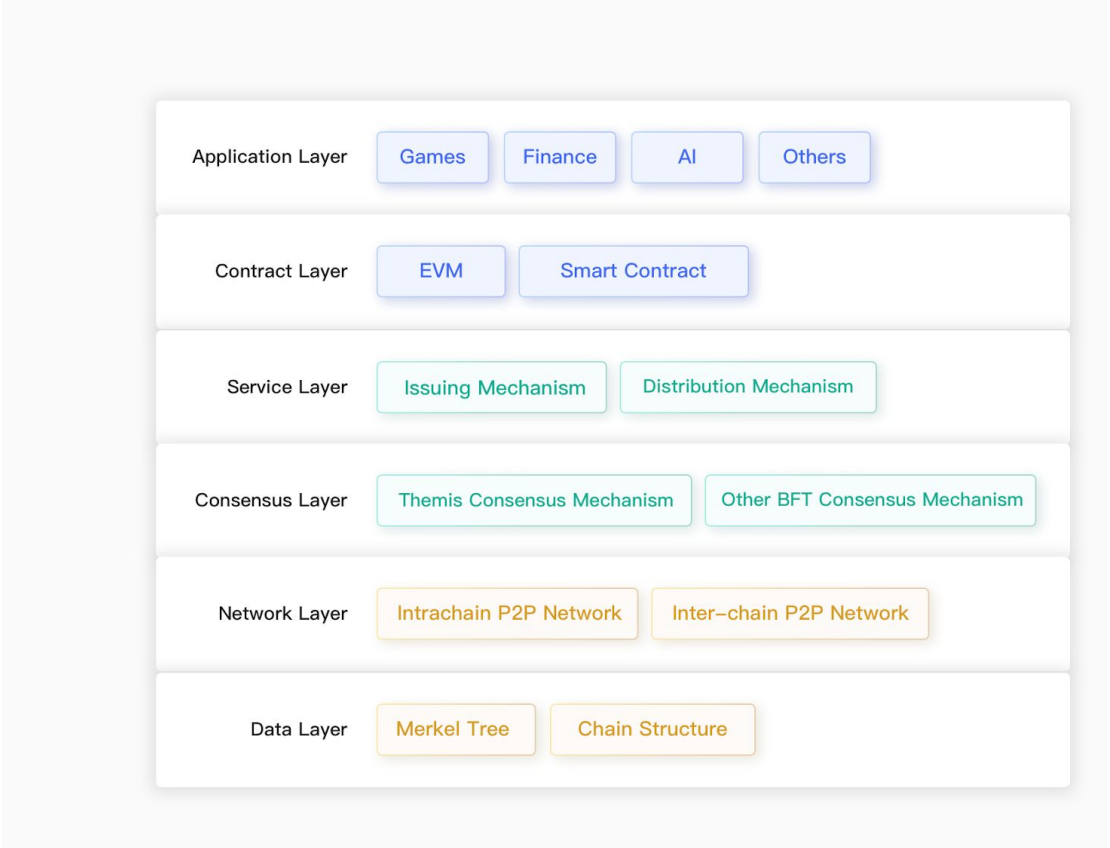
3. The Aurora Chain System Architecture

3.1 Schema Summary

In order to support DAPPs, the Aurora Chain has designed 6 layers. All applications are based on data, so the first layer of the Aurora Chain is dedicated to distributed data storage, not only to provide cheap, unlimited storage facilities, but also to ensure the data is absolutely safe, traceable and easy to use. The second layer is the P2P network system. The Aurora chain is ultimately a multi-chain blockchain platform. It has special requirements for network communication, which not only needs to meet the hierarchical communication within the chain, but also to quickly complete the consensus within the chain. The network is using a unique multi-protocol on a three-dimensional P2P network for a chain trading experience on the multi-chain blockchain platform. The consensus engine is considered the most important part of the blockchain, so we provide the consensus engine Themis in the third layer. The goal of this consensus engine is to solve the impossible triangle problem completely. Users want to build their own DAPP using the blockchain primarily with smart contracts and custom application platforms, therefore, the fourth and fifth layers have a variety of optional smart contract virtual machines, such as EWASM, EVM, etc., and some custom application interface based on the consensus engine which can meet the needs of various simple and complex DAPPs on the sixth layer.

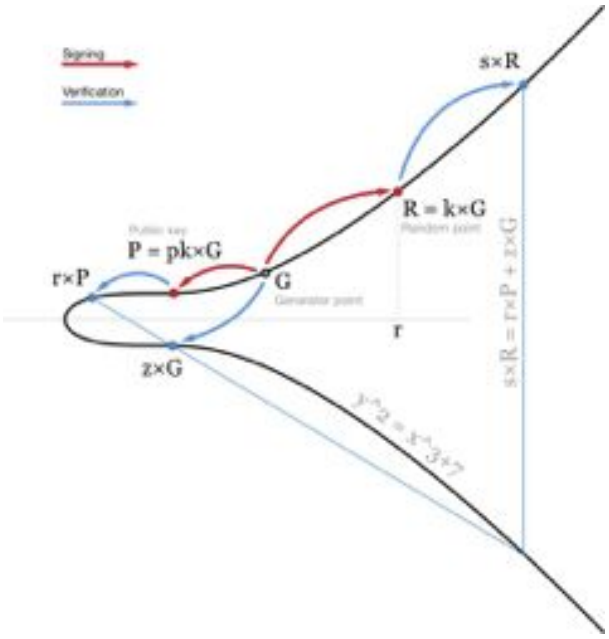
In order to better serve the application layer, Aurora strives to create a comprehensive blockchain infrastructure ecosystem to provide services based on blockchain digital virtual identity and credit reporting system on the fourth layer. Aurora offers a free open source wallet app, integrated blockchain digital virtual identity, blockchain asset custody, blockchain convenient payment and DAPP quick access SDK, allowing enterprise-level manufacturers to use Aurora on the basis of convenient blockchain services. This allows developers to complete the service of quick application publishing, sharing the Aurora community user resources, and enjoy the bonus of free traffic. Aurora offers more than just blockchain infrastructure, but a combination of blockchain solutions for games, finance, e-commerce, AI and big data.

3.2 Architecture Model



3.3 Protocols and Algorithms

3.3.1 ECDSA Elliptic Curve Digital Signature Algorithm



The ECDSA elliptic curve digital signature algorithm generates the public and private keys, and the secp256k1 curve is selected.

Select an elliptic curve Ep(a,b) and take a point on the elliptic curve as the base point G. Using the private key pk, we can generate a signature for the message m containing two numbers:

r (x coordinate of random point R = k × G)

s = (z+rpk)/k.

Then, using our public key P = pk × G, anyone can verify our signature by checking the x (s/s) × G + (r / s) × P x coordinates equal to r.

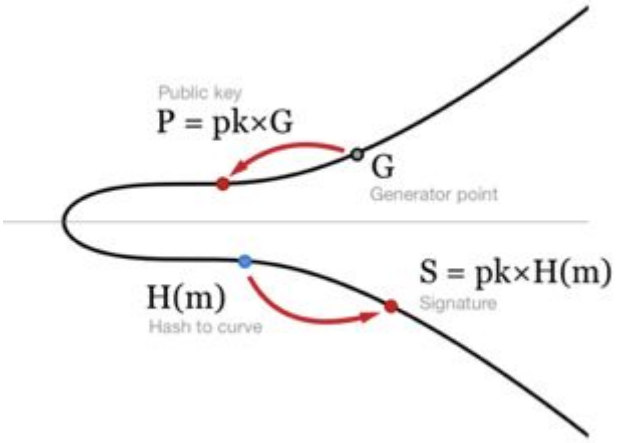
ECDSA cannot do signature aggregation or key aggregation, so only one signature can be verified. When verifying a multi-signature transaction, it is necessary to verify all the signatures and their corresponding public keys one by one, which consumes a large amount of block space and transaction costs.

3.3.2 BLS Signature Algorithm

BKS signature requires a random number generator that aggregates all the signatures in a block into one, making it easy to implement m-n multi-signatures and avoiding redundant communication between signers. In addition, the length of the BLS signature is shorter (the signature is a point on the elliptic curve instead of two).

We use pk for the private key, P = pk*G for the public key, and m for the message to be signed.

To calculate the signature, first curve the message H(m) and multiply the obtained result (curve coordinate point) by the private key: S = pk*H(m). You're done! No random numbers are needed, no extra steps are required, just multiply the hash result by the private key. The result of the signature is a point on the curve, saved in a compressed serialized format, which is only 33 bytes.



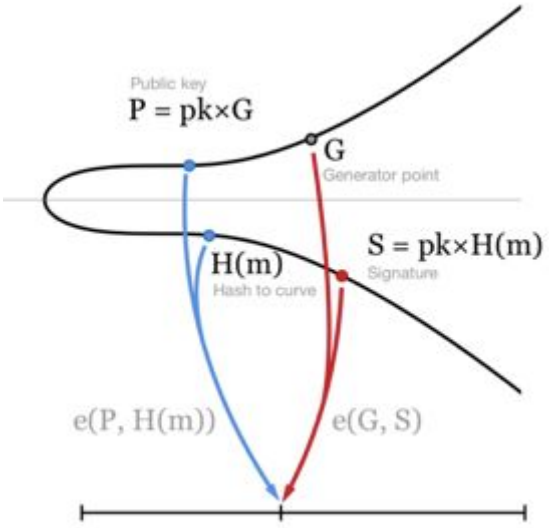
Generate a BLS signature. Multiply the hash result of the message by the private key.

We can use the public key P to verify the signature:

That is, e(P, H(m)) = e(G, S)

As mentioned earlier, the characteristics of the pairing function make the following equation true:

e(P, H(m)) = e(pk*G, H(m)) = e(G, pk*H(m)) = e(G, S)



BLS signature verification. We only need to verify that the public key and the hash of the message (two points on the curve) and the curve generation point and the signature (the other two points on the curve) map to the same number (if it is a valid BLS signature).

4. Aurora Chain Technology Features

4.1 Themis Consensus Mechanism

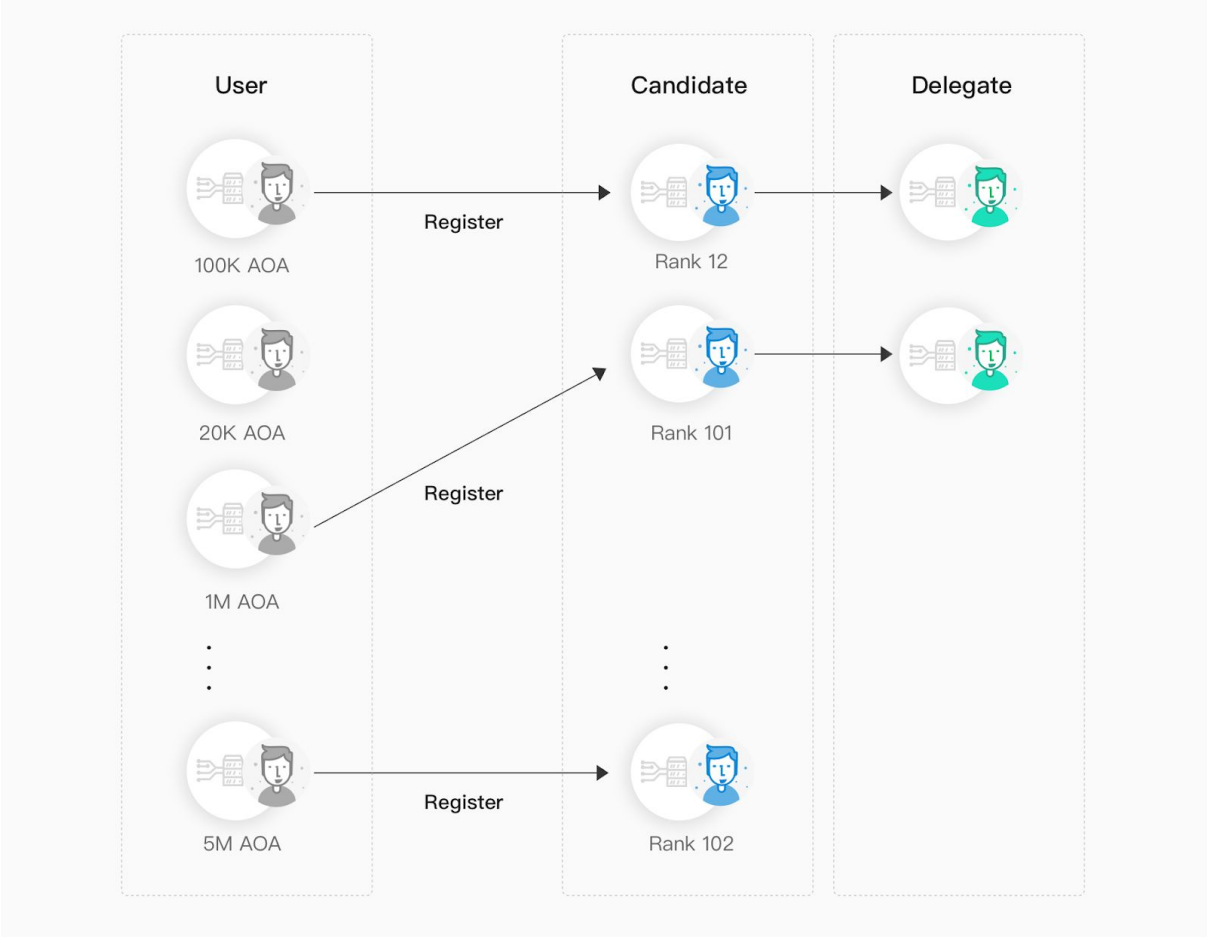
Existing blockchains make it difficult to achieve complete decentralization with simultaneous good system security, and high transaction processing capability. The designed consensus mechanism must have the advantages of low energy consumption, high efficiency, democratization, extremely low probability of divergence, and expandability, in an effort to solve the current limitations of blockchain technology in which an increase in a single area of functionality (e.g. scalability) requires a proportional decrease in other areas (security and stability, for instance)..

The consensus mechanism of the Aurora Chain is Themis, which achieves good security and superior processing power on the basis of maximum fairness and justice. The Themis consensus is a low-energy and efficient process that incorporates an improved version of the VRF, guarantees sufficient randomness, and eliminates non-human bifurcation.

Filter Delegate

The Themis Consensus Mechanism is done by delegates, which is divided into the production blocks Delegate and Validator. To become a Delegate, you need to register. Any user who has a certain number of AOA can register as a Candidate. Candidates can be voted

on by every address with an AOA, and the 101 Candidates with the highest number of votes automatically become Delegates. The Aurora public chain adopts the method of voting lock. The number of votes is equal to the number of AOA. After the voting is completed, the AOA will be locked in the user's own lock-balance until the user cancels the voting to retrieve the locked AOA. If the user votes with more than 1 AOA, then the user's Delegate block reward share is also obtained, and the split algorithm is dynamically calculated based on the voting status.



Random Block

In the process of generating blocks, a Delegate will randomly select a block to be the Production Delegate, and the rest will serve as Validators. To ensure safety and to foreclose cheating, the production block should be as unpredictable as possible when determining the order of Delegate work. The Aurora public chain incorporates an improved version of the VRF verifiable random function which offers a low cost, high efficiency, and sufficient randomness.

Untechnical Fork

Forking has always been a blockchain problem. In many cases, the longest chain is used to circumvent this problem, so there is a maximum number of confirmations. Themis has to pass at least 2 Validator verifications during the consensus process. A Block Delegate uses a standardized BLS signature to collect the correct signature of more than 2/3 Validator to determine a block correctness in advance, thereby reducing the blockchain acknowledgment to zero and eliminating non-human forks.

4.2 Upgradable Blockchain

The decentralization of the blockchain, coupled with the little need for upgrades in the early days, made the eventual blockchain upgrades difficult, and when they did occur, users often suffered unrecoverable losses. Today the internet is deeply rooted in the hearts of the people and most industries practice the concept of rapid iteration. Various industries can be restricted by blockchains that do not support rapid iteration. Such constraints may be fatal.

4.2.1 Upgradable Blockchain Summary

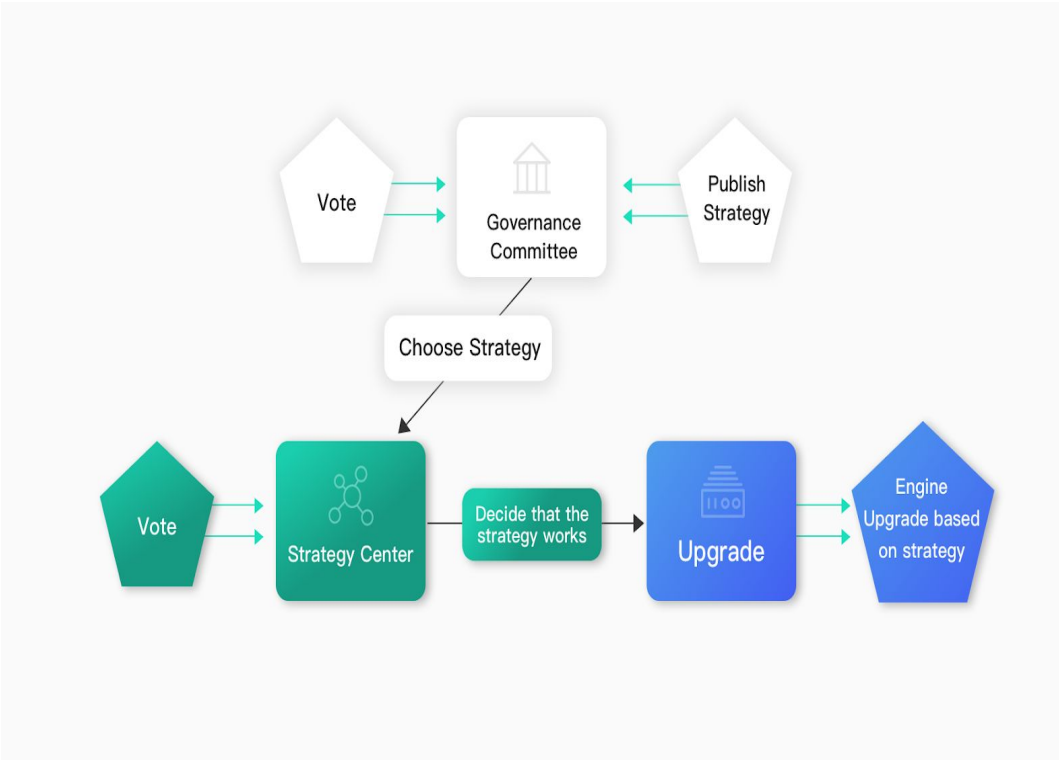
The Aurora blockchain will release the upgrade requirements in advance on the chain which will be voted by the whole community. After the vote has passed, it will be automatically upgraded to avoid losses to the users. The version update is intelligent, which can effectively reduce the risk of hard forks and improve the blockchain and contract scalability, adaptability, and usability.

The upgradeable blockchain requires the mining agent or candidate agent to vote on the upgrade blockchain in one polling cycle. When the upgrade vote exceeds two-thirds of the total number of voting agents and agent candidates, the upgrade is passed and the block height is then committed to implement the new upgrade.

The upgrade information includes the URL of the version released on GitHub, the version code, the update instructions, and the newly updated md5 information. When the upgrade program on the network receives an upgrade request, it will automatically retrieve the new version and continue to verify this version. After the verification is successful, the test network will be activated.

Users can experiment with new functionality on the test network. If an abnormal situation occurs, the agent that initiated the proposal can initiate a pause. After the suspension, if the upgrade altitude is reached, the suspension is not released, and the upgrade is invalid. If the suspension is lifted, the blockchain starts to upgrade normally.

4.2.2 Upgradable Blockchain System Architecture



The upgradeable blockchain consists of three modules: the governance committee, the strategy center, and the upgrade engine.

Governance Committee:

Decides via vote whether to release or replace the upgrade strategy.

Strategy Center:

Votes on the upgrade strategy to determine if the policy is executable. The detailed functions are as follows:

Mining agent or agent candidate initiates an upgrade vote

Other mining agents or agent candidates to vote

Vote will commence when more than 2/3 of the total number of votes are cast

The sponsor can suspend the upgrade

The initiator can resume the suspension of the upgrade

Upgrade Engine:

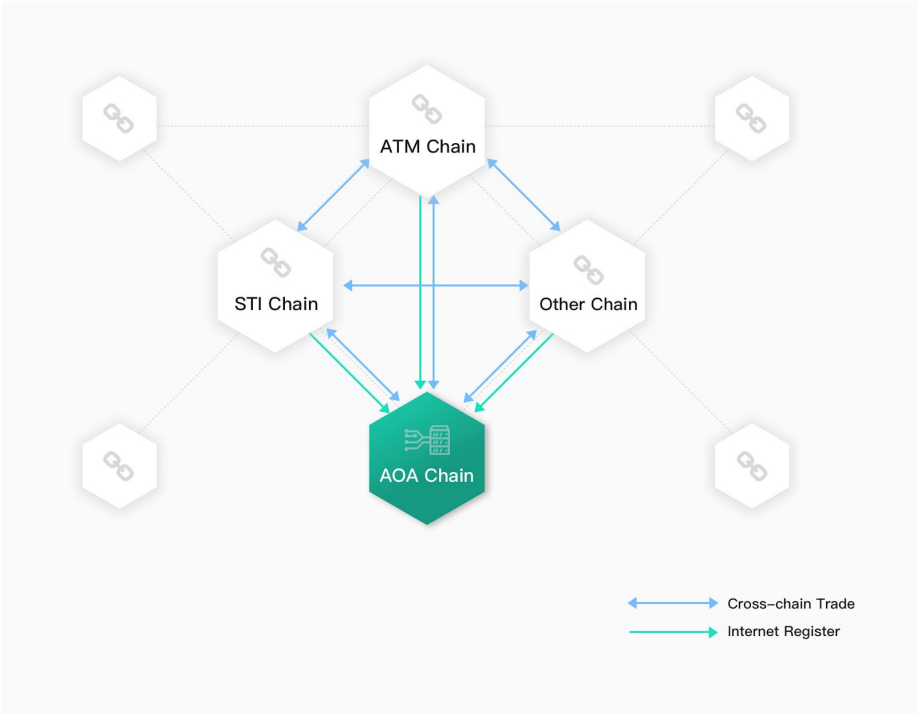
Manage the entire main chain, start, run, stop, upgrade process

Monitor the upgrade information and trigger the operation if you receive the upgrade related information.

Provide test network and official network parallel operation strategy

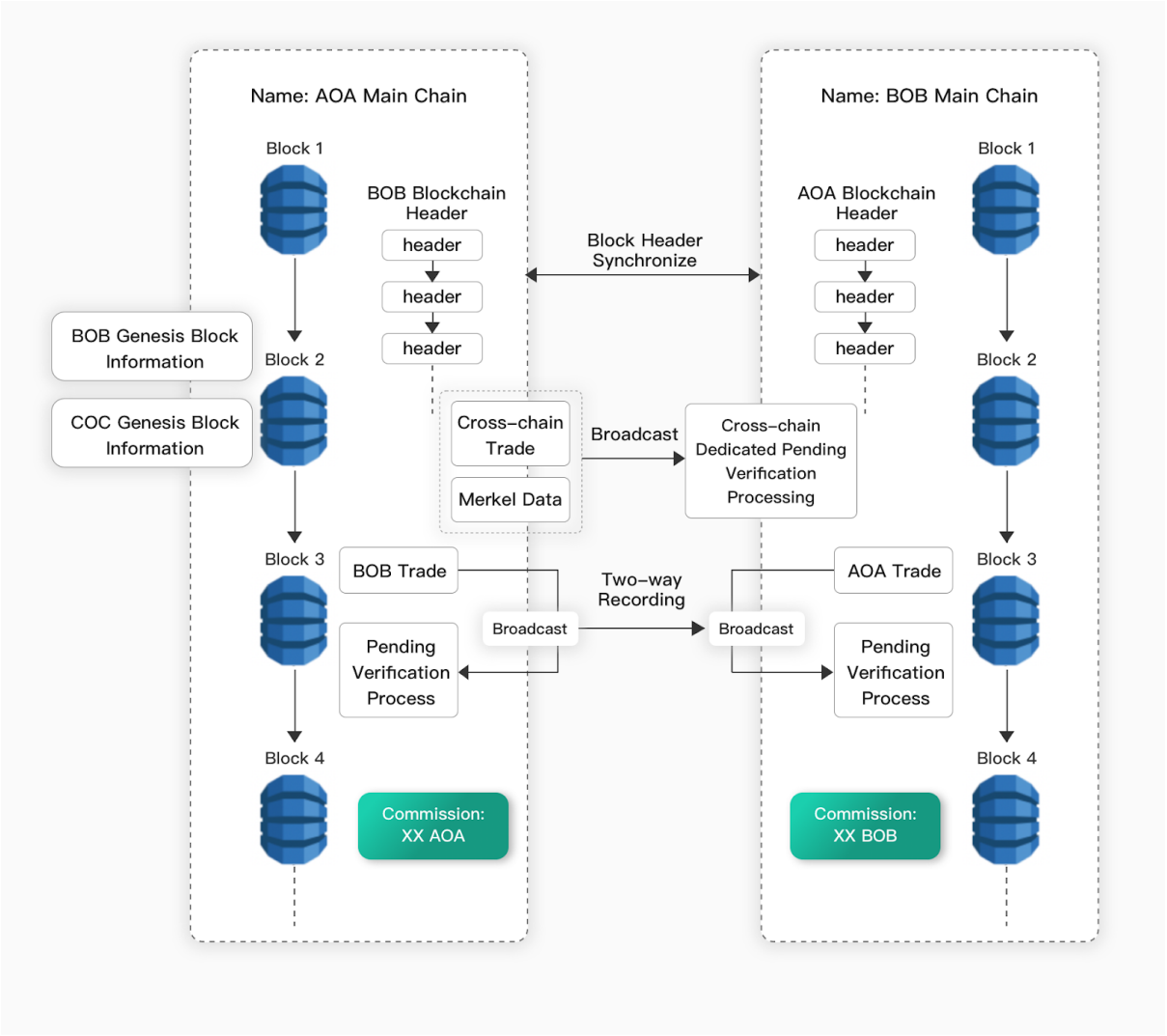
4.3 Multi-Chain Parallel Architecture

The existing blockchain technology is a single-chain architecture with one chain, one contract and multiple currencies. As more industries begin to adopt blockchain technologies, single chain architectures will inevitably contend with large bottlenecks in transaction performance, capacity, and scalability. Of the many multi-chain architectures in use today, we use a multi-chain network structure with the best isolation, performance, and scalability.



4.3.1 Parallel Chain

Parallel chain means that the chains in the network are independent and do not interfere with each other. Each chain has an independent consensus, independent contract, and independent storage. Any chain, in isolation, can run autonomously and completely, and only interact with other chains when cross-chain transactions and contract exchanges are required. The interaction of parallel chains is as follows:



Scalability

Parallel chain networks are infinitely scalable, especially in response to new demands. Due to the parallel nature of the chain, the newly added chain will not have any upgrades to the chain in the original network, only the new chain will follow the original network protocol standards.

Isolation

Good isolation is the primary feature of parallel chains over other chains. Any chain in the parallel chain is independent, which makes sure any chain is not affected by issues such as congestion or downtime on another chain. Quality isolation is an important criterion for measuring the maturity of a network system.

Multiple Consensus System

The consensus mechanism of the AOA backbone is Themis, but the multi-chain parallel network is an open blockchain network that supports more consensus mechanisms. In the process of integration with other industries, we have witnessed different consensus mechanisms in various industries, based on download volume, purchase volume, storage capacity, energy-based, and contribution-based multi-consensus system. The combination of blockchains and various industries has become easier.

It should be noted that in order to avoid the problem of collective fraud, the multi-consensus system of multi-chain parallel networks prohibits the forking or rolling back of the consensus mechanism on each chain.

4.3.2 Registration

When a chain needs to be connected to a multi-chain parallel network, it needs to be registered on the Aurora blockchain and to follow the relevant protocols of the multi-chain parallel network. Registration is open.

4.3.3 Unified Address System

One of the original intentions of multi-chain parallel network design is allowing users to receive and trade any asset in a multi-chain parallel network using only one address. This requires other chains in the network to use a unified address system, that is, the same private key. In different chains, the corresponding address is the same. For easy identification, different chains can use different prefixes to mark addresses.

4.3.4 Protocol Cluster

P2P Stereo Addressing Protocol

In a single-chain structure, any node is an equivalent entity, and an ordinary P2P network can be fully qualified for this task. In a multi-chain parallel network, a node of any chain can receive and forward messages of other chains, and the P2P stereo addressing protocol plays an important role in it.

Cross-chain Trading Agreement

The cross-chain transaction protocol is the core protocol of the multi-chain parallel network. It defines the whole process of cross-chain transactions, including the life cycle of the cross-link connection, transaction data packets, receipts and other information. Cross-chain protocols allow different tokens and standardized contracts to be moved between different blockchains.

Random Verification Protocol

In the design of multi-chain parallel networks, the interaction process of the two chains can randomly find a third-party chain for verification to ensure the authenticity of the transaction.

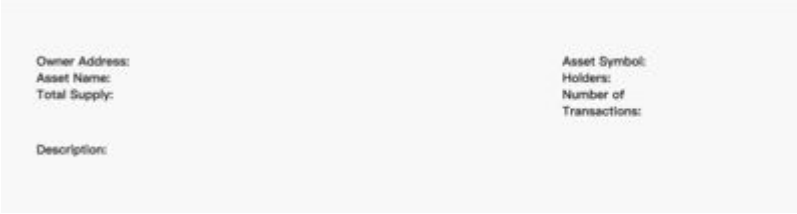
4.4 Digital Assets and Smart Contracts

In the face of the growing diversity of games and various applications, in order to provide better solutions for different developers, and to better and comprehensively meet the needs of different types of developers, Aurora Chain currently supports Aurora Chain Assets and Aurora Chain Smart Contract are two ways for developers to choose the way that suits them better.

4.4.1 Aurora Chain Digital Assets

Developers can quickly distribute and use tokens on Aurora Chain. The cost of issuing tokens in this way is extremely low, requiring only 0.0004 AOA. The threshold is low and there is a ready-made high-security complete code that can be used as a reference. Developers can easily publish tokens by providing basic information such as a token name, circulation, and description.

This method is more suitable for the use of Token as an application or in-game currency, points, etc. It has the advantages of low development difficulty, low commission, fast transfer speed, high security, etc. This solution can satisfy the basic needs of developers and users.



4.4.2 Aurora Chain Smart Contract

Aurora Chain uses the same Solidity version as Ethereum and is compatible with Ethereum EVM, fully supporting Ethereum ERC20, ERC-721 and other standard protocols. In this way, developers don't have to learn a new development language. Using known languages, developers can focus on work without having to switch between smart contracts. The EVM contract can be run in the sandbox of the Aurora Chain and interacts with the Aurora Chain application with a small amount of adaptation. In this way, the games or applications supported by Ethereum can be applied to the Aurora Chain relatively quickly.

Developers can customize and personalize related functions according to their own requirements. For example, apps or in-game items, equipment, and other assets can be implemented through the Aurora Chain, making it the only asset similar to the ERC721.

In short, Asset satisfies the developer's most basic Token release requirements, and Contract further satisfies the needs of developers to customize smart contracts.

5. Token

5.1 Token Economy

AOA is a common platform of the Aurora blockchain ecosystem, that provides a range of services including voting and payment and settlement of modules in the Aurora Ecology.

The value of AOA is predicated on:

1. Developing, certifying applications, and using chain services on the Aurora Chain requires payment of AOA. Access to various BaaS services in the Aurora ecosystem, including AuroraDev, AuroraDist, etc., also consumes AOA.
2. For Aurora C-terminal services users, AOA will serve as an important means of payment. In the following situations: : the use of financial services, such as cross-border payment, e-commerce platforms, supply chain and logistics financial services, etc. all need to use AOA for settlement; further, the services provided by the chain DAPP, such as blockchain games will be bought and sold with AOA; finally, all community work undertaken to build the ecosystem will use AOA as the main medium of circulation.
3. In the Aurora ecosystem, AOA can be obtained by offering products, services or interactions, for a range of industries.

5.2 Aurora Chain Applied to Blockchain+Gaming

Traditional game promotion channels connect game makers and operators, while recommending games to players for revenue. However, the game data of the player is only stored at the service end of the operator, and the evaluation of the effect of the game promotion channel is highly dependent on the trust relationship with the game operator. In this process, the game promotion channel may create false data in order to obtain higher profits. In addition, the game promotion channel cannot obtain the real promotion efficiency feedback, which leads to declines in efficiency. Games developed on the AuroraDev platform require that rules be approved by the community and users. Such transparency ensures that players' interests are protected first and foremost.

Traditional games are not linked to the player's economy, and money is earned by developers and publishers. The Aurora Eco-game offers opportunities for players to earn AOA through contributions that expand the community and for referrals. Earning and holding more AOA is further incentivized in a system that awards users one vote for each token held. Put simply, holding larger numbers of tokens translates into stronger voting power where players can determine the rules for both game play and the economic direction of the game core.

When AuroraDist diverts decentralized games through the intelligent distribution engine, it will charge a certain percentage of AOA based on the specific traffic imported. The props, equipment and other assets in the game can be converted into AOA. Users can trade AOA at AuroraDex which levies a small transaction fee.

It should be noted that the revenue of the game is divided into segments. After deducting labor costs and the server operation and maintenance costs, the surplus profits will be used to buy back AOA tokens held by users. The repurchase is designed to allow players with AOAs to enjoy the value of AOA's total liquidity deflation.

Aurora will offer new management and incentives as well as a multi-level referral system allowing players to earn both revenue in games and social events, and commissions from other players' payments. The system will reward AOA tokens to users and developers for contributing to the platform.

5.3 Aurora Chain Applied to Blockchain+Commerce

Traditional business points can only be transferred within the merchant, while AOA can be exchanged across merchants or platform transactions, and even share the value of the appreciation, but the AOA used only for trading can not fully stimulate the maximum capacity of the “token".
Suppliers, merchants, and buyers in the Aurora chain ecosystem can establish contacts and conduct transactions through smart contracts. After any user has agreed a deal, both parties can pay the AOA directly without having to go through a third-party intermediary. Users can get an AOA by posting an item or service on the trading platform, or they can use AOA to pay for products and services. The system is built to reduce friction in the transaction process, to increase transaction speeds and save transaction costs.

Although transactions are transparent on the blockchain, privacy protection can still be achieved. The blockchain account only holds AOA and ID transaction records, and real user data is managed by the decentralized application, which is completely controlled by individual users. At the same time, decentralized applications can support anonymous e-commerce platforms and anonymous product listings, allowing buyers and sellers to complete transactions with AOA in an anonymous situation.

AOA can be used as a vote. If an e-commerce company builds a DAPP in the Aurora ecosystem, it can mobilize the power of the community to resolve disputes. For example, community members can voluntarily become arbitrators, and arbitrators have the opportunity to receive AOA awards. Blockchain data is tamper-proof, and so bills, authenticity certificates, etc. on the blockchain can be referenced by an arbitrator. At the same time, the time-delay smart contract can provide AOA escrow services. Once the dispute is resolved or payment is agreed, the AOA will be automatically paid to the winning party, and all the arbitrators who support the winner will receive a corresponding proportion of the reward.

6. Governance

6.1 The Aurora Chain On-chain Governance Model

6.1.1 Elections

Under the Themis consensus mechanism, the Aurora chain production block can only be performed by 101 proxy nodes. Users can register as candidates and vote for the top 101 nodes with the highest number of votes through community voting.

6.1.2 Rewards

The agent node obtains the block reward every time the block is produced, and the user who votes for the agent node also gets the Delegate block reward share. The split algorithm is dynamically calculated according to the voting situation.

6.2 Parallel Chain Governance

Aurora's multi-chain system allows any one of the registered blockchains to communicate with each other. This communication mechanism and registration mechanism does not require other chains to be governed in the same way as Aurora, nor does it have any governance over other chains. Other chains are free to choose their own governance model.

6.3 Interchain Exchange

When two chains in the Aurora multi-chain system interact, the initiating party must pay a transaction fee (if any). No costs are borne by the receiving party.

6.4 Governance Upgrade

With the development of the Aurora blockchain ecosystem, the governance system can be upgraded after passing a community vote.

7. Technical Roadmap

May, 2018
Aurora chain on-line, synchronous online intelligent contract platform

December, 2019
Implement upgradeable blockchain, build AuroraDev, AuroraID

December, 2020
Complete multi-chain parallel system, build AuroraDist, AuroraDex, AuroraPay

December, 2021
Mature Aurora ecosystem

8. Glossary

Smart contract:
A smart contract is a computer protocol designed to disseminate, verify, or execute a contract in an informational manner. Smart contracts allow for trusted transactions without third parties, which are traceable and irreversible.

Consensus mechanism:
The 101 Proxy Nodes are responsible for establishing consensus. Since network-wide consensus is not required, the verification and confirmation of transactions can be completed in a short time.

Wallet:
A file containing a private key. It usually includes a software client that allows access to transactions that view and create specific blockchains designed by the wallet.

Block:
In a blockchain network, data is permanently recorded in the form of files, which we call blocks. A block is a set of records for some or all of the most recent transactions and is not recorded by other previous blocks.

Decentralized application:
The essence of DAPP is actually a protocol, a script written in code that runs automatically, stores its data on a blockchain, facilitates transactions with a cryptographic token, and operates on a protocol that displays valuable proof. And these codes are open source, can be seen by everyone, and cannot be modified at will.

Upgradeable blockchain:
Technical solutions designed to effectively reduce the risk of hard forks while improving the scalability, adaptability and usability of blockchains and contracts.

Cross-chain technology:
Bridges connecting the blockchains are designed to achieve atomic trading, asset conversion, and inter-blockchain interoperability between blocks.

Hard fork:

Blockchains have permanent differences. After new consensus rules are released, some nodes that have not been upgraded cannot verify the blocks produced by the nodes that have been upgraded. At this point, hard forms are usually implemented.

TPS:
Transaction Per Second, the number of services the system can process per second.

Solidity:
Is a high-level language with a syntax similar to JavaScript. It is designed to generate Ethereum virtual machine code in a compiled manner. Solidity facilitates the creation of contracts for voting, crowdfunding, closed auctions, multi-signature wallets, and more.

Decentralized Game Asset Exchange:
The platform will build a virtual property database. The props, tokens, and circulation paths held by gamers will be recorded on the chain. The Token and digital props in the Aurora Chain blockchain game ecosystem can be directly transacted across the platform.

Virtual Machine:
Refers to a complete computer system that implements a complete hardware system function and runs independently in a completely closed environment through technical simulation. The main task of the blockchain virtual machine is to run smart contracts. Essentially, a blockchain virtual machine is a coded runtime environment.

API:
Application Programming Interface refers to the conventions and services that connect different components of a software system.

Digital identity:
Digital identity refers to the identity information of individuals, organizations, and things in the form of electronic data.

Node:
Node, a copy of the ledger operated by the participants of the blockchain network.

Turing complete:
Refers to a machine or device that can be used to simulate the function of a Turing machine (the prototype of a modern general-purpose computer). Turing-complete machines are equivalent in terms of computability.

Multi-chain parallel expansion:

Said of a system that has achieved multi-chain parallel processing, unlimited upgrade TPS. The Aurora Chain offers easy upgradeability through the storage of low-level de on the chain itself. If consensus is passed, upgrades can take place automatically at a specified height.

Themis:

Aurora's original consensus mechanism is named Themis, which is based on maximum fairness and impartiality to ensure security and superior processing power. The consensus process has low energy consumption and high efficiency, and the improved version of the VRF verifies that the random function guarantees sufficient randomness and eliminates non-human forks.