Aurora Chain White Paper

Abstract

Aurora Chain applies DPOS+BFT consensus mechanisms and contracts with “speed of light” operation rate to link industries such as games, big data, AI and IoT. Aurora Chain’s slogan is to build a wonderful and colorful Blockchain world shining like aurora. Aurora Chain offers intelligent application isolation and enables multi-chain parallel expansion to create an extremely high TPS with security maintain. In this way, Aurora Chain ushers in a breakthrough into the Blockchain world.

To accomplish this mission, Aurora Chain has developed a number of techniques: DPOS+BFT consensus mechanisms can lower the risks of forking based on fast-working consensus mechanisms; P2P Stereo-net enables fast and secure communications by network layering; proprietary application isolation and Pending Zone intelligent regulation ensures that no inter-effects happen between the applications; multi-chain parallel operation and horizontal expansion enable unlimited increase of TPS; multi-asset launching simplifies the procedure of asset launching and provides high processing speed and the capability to expand to same level as the main chain coins; upgradable blockchain supports automatic upgrading; cluster self-grouping technology enables verification of transactions and downsizes users’ costs of data storage.

Aurora Chain commits itself to increasing operation speed and to create a blockchain technology born for applications. It does so by providing a solution to many common blockchain difficulties. Aurora Chain will help link all industries, promote the creation of applications, and build a colorful Blockchain world!

Content

Chapter One Background Information of Aurora Chain

Blockchain is a new distributed-infrastructure and computing-paradigm. It uses the block-chain data structure to verify and store data, the distributed-node-consensus algorithm to generate and upgrade data, cryptography to safeguard the process of data transmission and data access and smart contracts, consisting of automated scripts to write codes and process data.

Blockchain symbolizes a beginning of reliable Internet environment. Blockchain is attractive for trust can be built peer to peer on the network, making the value-transmission process transparent and confidential without intervention from intermediaries. This mechanism is co-determined but it can also protect individual rights, making the value exchange more efficient and less costly.

Chapter Two The Mission of Aurora Chain

Aurora Chain holds the mission of creating lightning fast contracts and facilitating the easy creation of applications on the blockchain.

Our central goals are as follows:

Focus on incorporating Blockchain into other industries

For now, Blockchain is most commonly used for digital asset offering. What Aurora Chain creates enables in-depth collaboration with other industries. Aurora Chain strives to allow businesses embed applications and rules into the Blockchain. Aurora Chain is born for applications, supports implementation of applications and can link disparate industries.

Focus on making the perfect smart contract

The smart contract is indispensable to incorporate Blockchain into other industries. How supportive a public chain is to contracts is closely related to how closely Blockchain is combined with other industries. Only contracts with an abundant underlayer, a high level of freedom and transparent code can meet the needs of different industries.

Focus on boosting the speed

People have long been criticizing that the transaction throughput（TPS）of many Blockchains hinders it from being combined with other industries. To allay this concern, Aurora Chain is focused on boosting the speed of transaction processing.

Focus on solving blockchain difficulties

Aurora Chain commits itself in building upgradable blockchain and realizing automatic upgrading in designated height. Meanwhile, with cluster self-grouping technology, Aurora Chain is able to reduce users' data storage costs. Aurora Chain offers resolution to difficulties when implementing blockchain technology in applications and speeds up the construction of blockchain ecology.

Ensure immediate application

Aurora Chain places emphasis on the combination of ideal and reality, the co-existence of efficiency and practicality. Aurora Chain enables in-depth incorporation with various types of applications to speed up the implementation of blockchain applications.

Chapter Three Technical Realization of Aurora Chain

The DPOS plus BFT consensus mechanisms

1.1 DPOS

Due to high transaction speed and high TPS of DPOS consensus mechanism, more and more blockchain projects are using DPOS（Delegated Proof of Stake） consensus mechanism. Aurora Chain also uses the DPOS mechanism.

When AOA balance of an account is higher than 5 million AOAs, the account can apply for the candidacy of AOA proxy; when AOA balance of a proxy candidate is lower than 5 million AOAs, its candidacy will be automatically disqualified; every address with balance of AOAs is qualified to vote for proxy candidacy and the top 101 candidates with the largest number of votes can automatically become the proxy nodes for packing transactions; Every address can only vote for each candidate once with maximum quotas of 101 votes. With one vote, 1 AOA needs to be locked till the end of voting.

1.2 BFT (Byzantine Fault Tolerance)

1）Adding BFS to DPOS can effectively avoid forks. Speed is greatly increased since there's no need waiting for N confirmation numbers after the block generation.

2）Aurora Chain builds up a stereoscopic P2P network where there is a broadcasting network among nodes based on UDP and a long connection among proxy candidates based on TCP. Through the upper network, a high-speed BFT consensus system can also be realized among proxy candidates.

3）A proxy ROOT tree is added to the head of each block to record its status and to boost the speed of verification.

The smart contract

Nick Szabo, a cross-field law scholar, defines the smart contract as a set of digital promises and protocols based on which shareholders keep these promises.

The smart contract is a program running on the Blockchain database used to process information and to get and send values.

Aurora Chain applies EVM virtual machine and Solidity developing languages to write smart contracts. In the future, Aurora Chain will support smart contracts based on Java, Go, and C++ among others.

P2P Stereo-net

A broadcasting network is built among different nodes. Proxy candidates can build up direct connection through the upper layer network which enables that BFT mechanism between proxies could be realized quickly. With network layering, we can achieve faster and safer communication.

Intelligent application isolation technology

Verified transactions will be processed in the Pending Zone. Proxy nodes pack transactions in the Pending Zone until let out.

Major functions of the smart scheduling pending area are as follows:

1. From a macroscopic view, it distinguishes contracts with different fees, flows and categories. It also takes a dynamic control of transaction's entering the Blockchain to make sure the process is fair and that clog of some contracts won't affect others.

2. From a microscopic view, it can monitor each contract in real time and make adjustments according to the real situation. It makes Blockchain more efficient and protects it from outside attacks.

Multi-asset offering

Procedure of asset offering can be simplified, with provision of processing speed and capability of expansion with the same level as main chain coins. The standard token offering procedure offers includes simplified and regulated token offering methods and procedures. With multi-asset token offerings, tokens can be used in the contracts directly and there is no need for introduction of other contracts.

The multi-chain parallel technology

The multi-chain structure makes transaction process more efficient than the single-chain structure for the latter is restricted by encryption algorithms and online transmissions. The stereoscopic P2P network can realize a cross-chain consensus system and increase TPS. Therefore, the ability of Blockchain can be infinitely increased as the number of chains increases.

The upgradable Blockchain

It's hard to upgrade Blockchain after it has been released except when a compulsory fork is applied at the expense of impeding the development of Blockchain. But with the LLVM compiler, Blockchain code and contract scripts will be put together. All clients will upgrade together after the upgraded Blockchain is placed on the old version at a specific link.

Cluster self-grouping

When any node turns on self-grouping function, certain nodes in the network will form up a cluster combination which can participate in transaction verification and storage to reduce users' data storage costs. By helping others with transaction verification, users will receive an extra bonus, which resembles a mining mechanism.

The anti-quantum-attack technology

The quantum calculation has a nature of concurrency due to the special characteristic of quantum information. For instance, when a quantum computer is processing an n-quantum-bit data, it is actually dealing with 2n data status. Due to their concurrency, quantum computers can solve problems not able to be solved by electronic computers. Therefore, the security of the current public-key system based on the

complexity of calculation is challenged by the powerful computing ability of quantum computers.

Two most common quantum algorithms used to decode are the Grover algorithm and the Shor algorithm. The Grover algorithm can cut length of the key by half while the Shor algorithm can attack common key agreements such as RSA, EIGamal, ECC and DH. Therefore, it's no longer secure to take RSA, EIGamal, ECC and DH as an encipher under the environment of quantum calculation.

Internationally, researches on the anti-quantum cryptography mainly focuses on the lattice-based cryptography, the code-based cryptography, the multivariate cryptography and the hash-based signatures cryptography.

The central problem of the lattice-based cryptography is the Shortest Vector Problem(SVP), that is to find the shortest non-void vector in the lattice system. Up to now, no quantum algorithm can decode the lattice-based cipher which is secure even under the worst condition. Out of a safety concern, Aurora Chain applies the lattice-based cryptography to cope with potential quantum attacks.

The cross-chain communications

Currently, it's still impossible for block chains are to communicate with each other. The isolation prevents different block chains from working together and impedes their development. Aurora Chain, however, supports a cross-chain communication protocol and other cross-chain technologies to ensure an unrestricted value-network.

The differentiated mining mechanism

On the Bitcoin network, mining nodes pack transaction records independently into new blocks through the workload management approach and get Bitcoins as a reward. The core of mining is to reward community members according to their contributions and therefore to encourage their participation.

Aurora Chain gives rewards to anything making contributions to the community such as upgrading the code, finding bugs, giving optimizing suggestions and spreading knowledge as long as they are recognized by the community members. The mining system won't be written into the Blockchain in the beginning. Instead, it will be tested and optimized in the community until the rules are finalized to maximize incentives.

The AOA Token and commission

AOA serves as the token to ensure Aurora Chain's proper functionality. Normally the commission rate of AOA is only 0.0001 except when it surges to protect the system from attacks.

The total volume of issuance of AOA tokens is 10 billion, among which 26% is for early community members, 34% for investors and partners and 40% for Aurora Foundation with purposes of use for daily operation, rewards for core team members and community developers as well as eco-system creation.

Chapter Four Background for Application of Aurora Chain

Application in the game industry

1.1 Blockchainization of the game tokens

Blockchain tokens are used in games for production, transaction and account settlement. They can be transformed in different games. In this open economic system, owners take a complete control of their tokens.

1.2 Blockchainization of the game data

Game props, characters and equipment are all defined by tokens. Tokens represent ownership so players can trade outside the games. Blockchainization of game characters and equipment brings a revolution to games. Therefore, it's necessary that game developers, operators and publishers redefine their own positions in games as a response to the change. Games will finally be community-based where rules of producing and consuming the equipment are co-determined by players and developers. Under this condition, games will grow more popular and have an extended life span.

1.3 Blockchainization of game rules

Blockchainization of game rules ensures a transparent production of game props and equipment that game developers or operators can not change. The sheer transparency attracts a lot of game players but also brings about challenges to game developers.

Application for the Internet of Things

The current Internet of Things system depends on a centralized network management architecture where all devices are connected through a cloud server. But in a decentralized Internet of Things system, Blockchain can create a basic framework to facilitate the transaction and cooperation of devices. Each device on the network functions as an independent, micro business entity.

Application in high-tech areas such as AI and Astronautics

In high-tech areas such as AI and astronautics, it's always a difficulty to balance the data security and the data synergy. The currently adopted centralized data network has problems collaborating across a cross-area system and a multi-node system. At the same time, collaboration among different data network systems is also not fully realized. Blockchain could be create a technological revolution for the IoT area.

Application in the Supply Chain Industry

Blockchain data is transparent and is shared by all parties. It forms a complete, fluent data flow on the whole service chain to make sure problems can be found and solved in time. Therefore, it can make the service chain management more efficient.

Chapter Five Roadmap of Aurora Chain

2018.3 Aurora Chain comes online and simultaneously opens the platform for smart contracts.

2018.5 We upgrade the intelligent application isolation technology and the Stereo-net, further improving security and operation speed.

2018.12 We complete a matured development of multi-chain parallel operation services, cluster grouping technology and upgradable blockchain technology, implementing cooperation between 30 applications.

2019 and beyond Realizing anti-quantum attacks and a Blockchain world that is more secure and faster. In effect, a more colorful blockchain world is created.

Chapter Six Website & Contact Information

Website: www.aurorachain.io

Email: official@aurorachain.io