Aster Smart Chain

WHITEPAPER ver. 1.2

DISCLAIMER: Nothing herein constitutes legal, financial, business, or tax advice, and you should consult your own legal, financial, tax, or other professional advisor(s) before engaging in any activity in connection with this. The Aster Smart Chain team nor any of the project team members who work or have worked on the Aster Smart Chain project (as defined herein) in any way whatsoever, nor any third-party service provider, shall be liable for any kind of direct or indirect damage or loss whatsoever which you may suffer in connection with accessing this whitepaper, the website, Twitter, Telegram, or any other websites or materials published by the company. This whitepaper does not encourage investment in the Aster Smart Chain project. Please do your own research and follow up on the project.

Aster Smart Chain Foundation

Created on April 10th, 2023

Updated on September 27, 2024

1. Introduction

1.1 Vision

ASTER is an ambitious project committed to creating a fully decentralized internet and its supporting infrastructure. As one of the largest blockchain-based operating systems globally, the ASTER Protocol delivers high throughput, scalability, and availability for all Decentralized Applications (DApps) within its ecosystem. In September 2024, the addition of Kronobit Networks' assets to the Aster Chain introduced a new, trusted option for holders, expanding the platform's usability and trustworthiness.

1.2 Terminology

Address/Wallet

An address or wallet consisting of account credentials on the ASTER network are generated by a key pair, which consists of a private key and a public key, the latter being derived from the former through an algorithm. The public key is usually used for session key encryption, signature verification, and encrypting data that could be decrypted by a corresponding private key.

ABI

An application binary interface (ABI) is an interface between two binary program modules; usually one of these modules is a library or an operating system facility, and the other is a user run program.

API

An application programming interface (API) is mainly used for user client’s development. With API support, token issuance platforms can also be designed by developers themselves.

Asset

In ASTER's documents, asset is the same as token, which is also denoted as AST-20 token.

Block

Blocks contain the digital records of transactions. A complete block consists of the magic number, block size, block header, transaction counter, and transaction data.

Block Reward

Block production rewards are sent to a sub-account (address/wallet). Super Representatives can claim their rewards on Asterscan or through the API directly.

Block Header

A block header is part of a block. ASTER block headers contain the previous block’s hash, the Merkle root, timestamp, version, and witness address.

Cold Wallet

Cold wallet, also known as offline wallet, keeps the private key completely disconnected from any network. Cold wallets are usually installed on "cold" devices (e.g. computers or mobile phones staying offline) to ensure the security of AST private key.

DApp

Decentralized Application is an App that operates without a centrally trusted party. An application that enables direct interaction/agreements/communication between end users and/or resources without a middleman.

gRPC

gRPC[2] (gRPC Remote Procedure Calls) is an open source remote procedure call (RPC) system initially developed at Google. It uses HTTP/2 for transport, Protocol Buffers as the interface description language, and provides features such as authentication, bidirectional streaming and flow control, blocking or nonblocking bindings, and cancellation and timeouts. It generates cross-platform client and server bindings for many languages. Most common usage scenarios include connecting services in microservices style architecture and connecting mobile devices, and browser clients to backend services.

Hot Wallet

Hot wallet, also known as online wallet, allows user's private key to be used online, thus it could be susceptible to potential vulnerabilities or interception by malicious actors.

JDK

Java Development Kit is the Java SDK used for Java applications. It is the core of Java development, comprising the Java application environment (JVM+Java class library) and Java tools.

KhaosDB

ASTER Smart Chainhas a KhaosDB in the full-node memory that can store all the newly-forked chains generated within a certain period of time and supports witnesses to switch from their own active chain swiftly into a new main chain.

LevelDB

LevelDB was initially adopted with the primary goal to meet the requirements of fast R/W and rapid development. After launching the Mainnet, ASTER upgraded its database to an entirely customized one catered to its very own needs.

Merkle Root

A Merkle root is the hash of all hashes of all transactions included as part of a block in a blockchain network.

Public Testnet

A version of the network running in a single-node configuration. Developers can connect and test Dapps and features without worrying about the economic loss. Testnet tokens have no value and anyone can request more from the public faucet.

RPC[3]

In distributed computing, a remote procedure call (RPC) is when a computer program causes a procedure (subroutine) to execute in a different address space (commonly on another computer on a shared network), which is coded as if it were a normal (local) procedure call, without the programmer explicitly coding the details for the remote interaction.

Scalability

Scalability is a feature of the ASTER Protocol. It is the capability of a system, network, or process to handle a growing amount of work or its potential to be enlarged to accommodate that growth.

Throughput

High throughput is a feature of ASTER Mainnet. It is measured in Transactions Per Second (TPS), namely the maximum transaction capacity in one second.

Timestamp

The approximate time of block production is recorded as UNIX timestamp, which is the number of milliseconds that have elapsed since 00:00:00 01 Jan 1970 UTC.

TKC

Token configuration.

AST-20

A standard of crypto token on ASTER platform. Certain rules and interfaces are required to follow when holding an initial coin offering on ASTER blockchain. The AST-20 is the standard Token creation

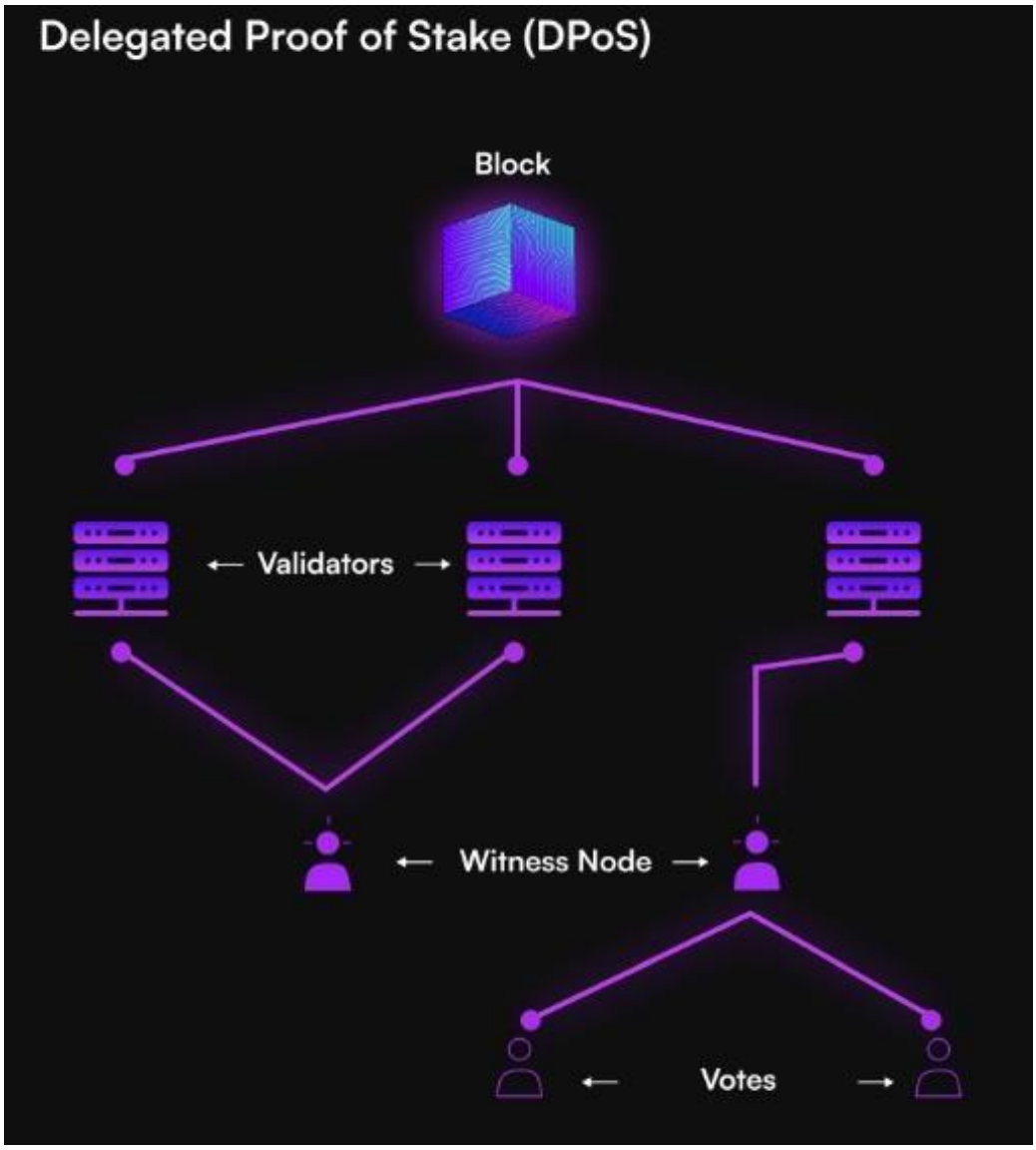
AST

AST stands for Aster, which is the official cryptocurrency of ASTER BLOCKCHAIN

2. Consensus

2.1 Delegated Proof of Stake (DPoS)

The old consensus mechanism is the Proof of Work (PoW) consensus mechanism. This protocol is currently implemented in Bitcoin[7] and old Ethereum[8]. In PoW systems, transactions broadcast through the network are grouped together into nascent blocks for miner confirmation. The confirmation process involves hashing transactions using cryptographic hashing algorithms until a merkle root has been reached, creating a merkle tree:



Cryptographic hashing algorithms are useful in network attack prevention because they possess several properties[9]:

- ***Input/Output length size*** - The algorithm can pass in an input of any length in size, and outputs a fixed length hash value.
- ***Efficiency*** - The algorithm is relatively easy and fast to compute.
- ***Preimage resistance*** - For a given output *z*, it is impossible to find any input *x* such that *h(x) = z*. In other words, the hashing algorithm *h(x)* is a one-way function in which only the output can be found, given an input. The reverse is not possible.
- ***Collision resistance*** - It is computationally infeasible to find any pairs $x_1 \neq x_2$ such that $h(x_1) = h(x_2)$. In other words, the probability of finding two different inputs hashing to the same output is extremely low. This property also implies *second preimage resistance*.
- ***Second preimage resistance*** - Given x_1, and thus $h(x_1)$, it is computationally infeasible to find any x_2 such that $h(x_1) = h(x_2)$. While this property is similar to *collision resistance*, the property differs in that it is saying an attacker with a given x_1 will find it computationally infeasible to find any x_2 hashing to the same output.
- ***Deterministic*** - maps each input to one and only one output.
- ***Avalanche effect*** - a small change in the input results in an entirely different output.

These properties give the cryptocurrency network its intrinsic value by ensuring attacks do not compromise the network. When miners confirm a block, they are rewarded tokens as a built-in incentive for network participation. However, as the global cryptocurrency market capitalization steadily increased, the miners became centralized and focused their computing resources on hoarding tokens as assets, rather than for network participation purposes. CPU miners gave way to GPUs, which in turn gave way to powerful ASICs. In one notable study, the total power consumption of Bitcoin mining has been estimated to be as high as 3 GW[10], comparable to Ireland's power consumption. This same study projected total power consumption to reach 8 GW in the near future.

To solve the energy waste issue, the Proof of Stake (PoS) consensus mechanism was proposed by many new networks. In PoS networks, token holders lock their token balances to become block validators. The validators take turns proposing and voting on the next block. However, the problem with standard PoS is that validator influence correlates directly to the amount of tokens locked up. This results in parties hoarding large amounts of the network's base currency wielding undue influence in the network ecosystem.

The ASTER consensus mechanism uses an innovative Delegated Proof of Stake system in which 47 Validators (Val) produce blocks for the network. Every 6 hours, AST account holders who freeze their accounts can vote for a selection of VAL candidates, with the top 47 candidates deemed the VAL. Voters may choose VALs based on criteria such as projects sponsored by Vals to increase AST adoption, and rewards distributed to voters. This allows for a more democratized and decentralized ecosystem. VALs' accounts are normal accounts, but their accumulation of votes allows them to produce blocks. With the low throughput rates of Bitcoin and old Ethereum due to their PoW consensus mechanism and scalability issues, ASTER's DPoS system offers an innovative mechanism resulting in 2000 TPS compared to Bitcoin's 3 TPS and Ethereum's 15 TPS.

The three types of nodes on the ASTER network are Witness Node, Full Node, and Solidity Node. Witness nodes are set up by VALs and are mainly responsible for block production and proposal creation/voting. Full nodes provide APIs and broadcast transactions and blocks. Solidity nodes sync blocks from other Full Nodes and also provide indexable APIs.

Staking Requirements for 47 Validators and 33 Delegates on Aster Smart Chain

Total supply of 575 million coins, here is a step-by-step allocation model for a DPoS network:

1. Reserve Supply for Staking

In a DPoS system, 40% to 60% of the total coin supply is typically reserved for staking, especially in the early stages. With a 50% staking reserve, which is ideal for maintaining a secure and active network, 287.5 million coins would be locked in staking.

2. Distribution per Validator and Delegate

Validators (47): Approximately 70% of the staking reserve can be allocated to validators, who handle most of the network's workload. This would amount to 201.25 million coins. Each validator would require approximately 4.28 million coins in staking.

Delegates (33): The remaining 30% of the staking reserve, or 86.25 million coins, can be distributed among delegates for operations and voting. Each delegate would require approximately 2.61 million coins in staking.

3. Final Considerations

Flexibility in Staking Requirements: Some networks allow staking requirements to vary based on community participation and network needs. Staking values can be dynamically adjusted to attract more participants or to control the number of validators and delegates. Staked coins are typically locked for periods of 1 to 2 years, helping ensure that validators and delegates are committed to the network for the long term.

The Circulating Supply = **287.5 million AST coins at Main network**
The Circulating Supply for Testnet **= 575 million AST (test)**

Whats the New concept of Aster Smart Chain to Blockchain world:

1. Cross-Chain Interoperability for DPoS Networks

- Description: Develop a cross-chain interoperability protocol that allows different DPoS chains to communicate and transfer assets seamlessly. This would enable greater scalability by integrating multiple DPoS ecosystems.
- Innovation: Facilitates smooth interaction between different DPoS networks, creating a more cohesive and versatile blockchain ecosystem.

2. Event-Based Adaptive Governance

- Description: A governance system that dynamically adapts to real-time network conditions or specific events, such as detecting malicious activity or drastic changes in transaction volume. Governance rules and policies would be automatically adjusted to mitigate risks or optimize performance.
- Innovation: Provides a flexible governance model that ensures the network is continuously adapting to new challenges or opportunities.

3. Tokenized Validator Insurance Pool

- Description: Introduce an insurance system for validators where a portion of the staking rewards is contributed to an insurance pool. This pool would cover losses for delegators in case a validator fails to meet performance or security standards.
- Innovation: Increases trust in validators and reduces the financial risk for delegators, improving network resilience.

4. Real-Time, On-Chain Dispute Resolution Mechanism

- Description: Build an on-chain system where validators or delegators can resolve disputes in real-time without requiring external mediation. The system would rely on smart contracts to automate arbitration and settlement of conflicts.
- Innovation: Enables quicker conflict resolution and eliminates the need for off-chain intervention, increasing transparency and trust.

5. Stakeholder-Driven Sidechain Creation

- Description: Introduce a system where DPoS token holders can vote to create sidechains with specialized functionalities (e.g., for privacy, speed, or specific dApp support). These sidechains would be governed by the main chain but operate independently for specific tasks.
- Innovation: Provides more customization and scalability by allowing stakeholders to tailor the blockchain infrastructure to their specific needs.

6. Dynamic Reward Redistribution Based on Network Activity

- Description: A reward system that adjusts the distribution of staking rewards dynamically based on overall network activity. During periods of high activity, more rewards would be directed to validators to incentivize better network performance.
- Innovation: Optimizes the reward structure to ensure that the network remains secure and efficient during peak usage times.

Staking Consensus Parameters

- MAX_VALIDATORS: 47

(Maximum number of allowed validators)

- MIN_STAKE: 150,000 AST

(Minimum amount each validator must stake to become a validator)

- MAX_STAKE: 5,000,000

(Maximum amount a validator can stake to become a validator)

- CYCLE_DURATION_BLOCKS: 48 hours

(Duration of each cycle in blocks, calculated as [48*60*60/5])

- DEFAULT_VALIDATOR_FEE: 15%

(The validator must stake at least the minimum amount to participate, with a default fee of 15%)

- BLOCK_REWARD_AMOUNT:

(Calculated as: (Total Supply * Inflation/100) / Blocks Per Year, where inflation equals APY, usually around 1%. This reward is shared among validators based on the proportion of their staking)

Aster Smart Chain Staking Rule

Within the DPoS protocol, there is a Staking system that is exclusive to validators & big quantity coin holders. This system is locked for a specified period of time, with a minimum of 1 year and a maximum of 5 years, during which dividends are paid to the owners at a rate of 2% to 5% monthly, depending on the established period. This ensures fairness for both owners and holders, allowing everyone to participate in this system.

The Bridge

Advantages of the Bridge between a Aster SmartC Chain and the BSC Blockchain

Enhanced Scalability
- DPoS Blockchain: DPoS chains are known for high scalability due to the use of a limited number of validators selected by the community.
- BSC: BSC offers scalable and fast capacity through its design, allowing efficient transaction handling.
- Bridge Advantage: A bridge between DPoS and BSC combines these advantages, increasing transaction processing capacity and expanding access across both networks.

Asset Interoperability
- DPoS Blockchain: Assets in DPoS chains, such as tokens or NFTs, can circulate within their own ecosystem.
- BSC: BSC allows smooth movement of assets between different chains through interoperability protocols.
- Bridge Advantage: Users can transfer assets between both chains, increasing liquidity and access to various tokens and enabling interaction between diverse dApps.

Cost Optimization
- DPoS Blockchain: Transaction fees in DPoS are typically low due to network efficiency, as a limited number of validators handle operations.
- BSC: BSC offers low-cost transactions with fast processing times.
- Bridge Advantage: A bridge between both networks allows users to benefit from low fees across both blockchains, enhancing transaction cost-efficiency and enabling users to choose the most economical chain for their operations.

Robust Security and Decentralization
- DPoS Blockchain: Validators in DPoS are elected by the community, introducing a high level of decentralization and rapid consensus.
- BSC: BSC has robust security measures, focusing on secure validation processes.
- Bridge Advantage: Connecting a DPoS blockchain with BSC improves security across ecosystems, allowing users to leverage the strengths of both networks and mitigate vulnerabilities.

Expansion of Markets and Users
- DPoS Blockchain: The community of a DPoS chain is typically centered around specific applications or use cases.
- BSC: BSC has a large user base with access to various projects and services.
- Bridge Advantage: A bridge between both blockchains allows users access to a broader range of dApps, projects, and markets, enhancing opportunities for adoption and business expansion for developers and users.

Governance and Community Decision-Making
- DPoS Blockchain: Validators and delegators in a DPoS chain actively participate in governance by voting on proposals.
- BSC: BSC is also implementing decentralized governance solutions.
- Bridge Advantage: The bridge could facilitate cross-chain governance, allowing users from both chains to participate in decisions, promoting broader community integration and consensus.

Accelerating Transactions for DeFi Applications and dApps
- DPoS Blockchain: DPoS enables faster block times compared to other consensus mechanisms like PoW, enhancing dApps and DeFi services.
- BSC: BSC is known for its quick transaction speeds, handling thousands of operations per second.
- Bridge Advantage: A bridge between both networks could support DeFi applications and dApps needing high transaction speeds, eliminating performance bottlenecks across platforms.

Improved User Experience
- DPoS Blockchain: Applications on DPoS networks generally offer user-friendly interfaces but may benefit from additional tools.
- BSC: BSC offers a great user experience and is widely accessible.
- Bridge Advantage: DPoS users could benefit from integration with BSC tools, improving accessibility and encouraging broader adoption.

Future Innovations and Joint Developments
- DPoS Blockchain: DPoS networks are constantly evolving with new improvement proposals and community-driven development.
- BSC: BSC continues to integrate advanced technologies and innovative solutions.
- Bridge Advantage: A bridge between both chains would foster collaboration and joint technological advancements, promoting innovation across both ecosystems.

Combined Staking and Reward Systems
- DPoS Blockchain: Validators and delegators earn rewards through staking.
- BSC: BSC has its own staking and validation mechanisms.
- Bridge Advantage: A bridge could allow users to participate in staking schemes on both networks, optimizing reward distribution and increasing validator participation.

In summary, a bridge between a DPoS Blockchain and BSC would enhance scalability, interoperability, and security, while providing users with a more flexible and rewarding experience in governance, staking, and transaction cost efficiency.

The Bridge between Aster Smart Chain will be Build and Hosted by:

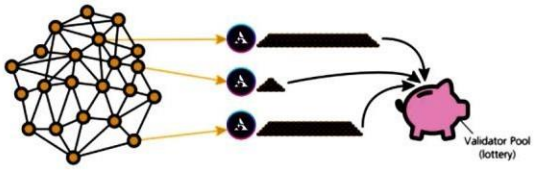
Coins Available inthe Bridge and Their Exchange Method:

Typically, cross-chain bridging steps occur within DEX/SWAP platforms, which can sometimes lead to congestion issues and occasional errors that require manual correction by a dedicated team. To address this, Aster Smart Chain will implement an independent cross-chain bridge, allowing for the exchange of the following coins:

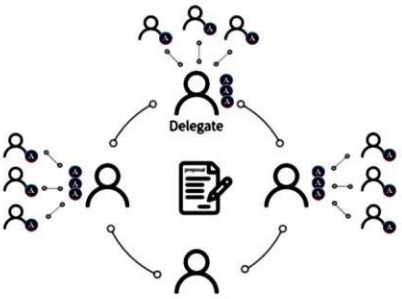
1- USDT BSC to USDT Aster Chain
2- USDC BSC to USDC Aster Chain
3- BNB BSC to BNB Aster Chain
4- AST BSC to AST Aster Chain

The handling and transfer of coins via the bridge are independent of all Dapps, meaning that transactions are made from the same wallet on two independent chains. In this case, the bridge will have no direct interaction with Dapps.

Difference between POS & Dpos



PoS



DPOS

Network Fee

ASTER network generally does not charge fees for most transactions, however, due to system restrictions and fairness, bandwidth usage and transactions do take in certain fees.

Fee charges are broken down into the following categories:

1. Normal transactions cost bandwidth points. Users can use the free daily bandwidth points (5000) or freeze AST to obtain more. When bandwidth points are not enough, AST will be used directly from the sending account. The AST needed is the number of bytes * 10 SUN.
2. Smart contracts cost energy (Section 6) but will also need bandwidth points for the transaction to be broadcasted and confirmed. The bandwidth cost is the same as above.
3. All query transactions are free. It doesn't cost energy or bandwidth.

ASTER network also defines a set of fixed fees for the following transactions:

1. Creating a witness node: 9999 AST
2. Issuing a AST-20 token: 0.000024 AST
3. Creating a new account: 0.1 AST
4. Creating an exchange pair: 1024 AST

Presale System

1. Platform:
Aster Smart Chain will implement its presale system on the Binance Smart Chain (BSC).

2. Single-Token Model:
The presale will operate under a single-token model:
- Tokens allocated for the presale are strictly reserved for presale purposes and the creation of the initial liquidity pool.

3. Total Supply:
- The total supply of Aster Smart Chain's blockchain is 575 million AST Coins.

4. BSC Supply:
- The total supply for Binance Smart Chain (BSC) is 275 million AST Coins.
- No additional AST tokens will be created on BSC. This ensures protection for the future bridge between both chains.

5. Token Allocation:
- These 275 million AST tokens are distributed between:
- The presale system.
- The initial liquidity launch on PancakeSwap.

Kronobit Blockchain Absorption

Aster Smart Chain has announced the absorption of Kronobit Networks as part of a strategic agreement between both parties. Under this agreement, Aster Smart Chain commits to integrating Kronobit Networks users through an assimilation process basedon the following conversion rates: **1,000,000 KNB = 300,000 AST and 1,000,000 XKR = 2,000 Aster Dex Native Token (TBA), with a maximum limit of 2,000,000 KNB and 2,000,000 XKR. The remaining Kronobit coins (KNB) will be exchanged and distributed every 30 days until the full snapshot is completed (Vesting Mode).**

These conversion rates have been set considering the differences in the total token supply between both networks, and Aster Smart Chain's locking system will be implemented. This ensures a fair and balanced transition for **KNB** and **XKR** holderswithin the Aster ecosystem without harming either party.

To prevent Kronobit users from being excluded due to forgetfulness or other reasons, one of the requirements to benefit from the Aster project is active participation in Aster Smart Chain campaigns such as "Airdrop, Pre-sale, Social Media Engagement, Posts, and more. **Kronobit holders must fill out a form with the following information: Telegramusername, email address (Gmail only), and the wallet address used in Kronobit.** This ensures that users cannot claim ignorance, as after **30** days from the start of the migration and closure process, no claims will be accepted, and the Aster team will not be able to assist.

Conclusion

ASTER SMART CHAIN is a scalable Blockchain solution that has employed innovative methods for tackling challenges faced by legacy Blockchain networks.

* TBA = To be Announced!

Aster Smart Chain is continuously growing, and new implementations will be added or modified as required by the project and/or regulations.