



APOLLO SMART CHAIN

COMPANY OVERVIEW

A company specialized in the field of blockchain and digital platforms and the owner of the first hybrid currency project in various digital fields, which will be released soon.

Projects

1-Apollo's secret conversation

2-Apollo Smart Chain

3-apollo-generator

4-Apollo-AI-Image

5-apollo-estate

6-Apollo Wallet

7-Apollo music

8-Apollo Swap

9-apollo-nft

10-apollo-ai



COMMUNICATION

[TikTok](#)



apollosmartchain@gmail.com



[Telegram](#)



WHITE PAPER

- Roadmap
- Token distribution
- Token Allocation Distribution

EXTRA WHITE PAPER



Apollo Smart Chain



Apollo Swap

All of these projects belong to one hybrid currency called ASC

Roadmap for the Digital Currency Project

Q1 - Q2 (Month 1 - Month 6): Foundation and Preparation Phase

1. Research and Strategic Planning - Conduct comprehensive market studies to identify gaps and strategic opportunities. - Analyze needs and budget, determine technologies to be used. - Duration: 1-2 months. 2. Building the Team and Establishing Strategic Partnerships - Hire a team of developers, blockchain experts, and legal advisors. - Connect with potential partners and initiate collaborations. - Duration: 1-2 months. 3. Project Structure Design and Prototyping - Create initial prototypes for the platform, wallet, and chat application. - Gather initial feedback from partners and investors to refine the design. - Duration: 2-3 months.

Q3 - Q4 (Month 7 - Month 12): Infrastructure and Core Technology Development

1. Development of Smart Contracts and Core Infrastructure - Design and develop smart contracts for the trading platform and wallet. - Build the infrastructure for the chat application and data encryption. - Duration: 2-3 months. 2. User Interface and User Experience (UI/UX) Development - Develop customized interfaces for the digital wallet, chat application, and token generation platform. - Enhance the user experience based on early user feedback. - Duration: 2 months. 3. Security Testing and Legal Review - Perform security testing across platforms (penetration testing, data confidentiality assurance). - Conduct legal review to ensure compliance with regulatory requirements. - Duration: 1-2 months.

Q1 - Q2 of the Following Year (Month 13 - Month 18): Beta Launch and Promotion

1. Beta Launch of Core Platforms (MVP) - Launch beta version of the trading platform, digital wallet, and chat application. - Collect user feedback and improve performance based on input. - Duration: 2-3 months. 2. Development and Launch of NFT and AI Platforms - Build an NFT platform operating on multiple networks, and develop AI for image generation. - Launch beta versions to attract early users and investors. - Duration: 3 months. 3. Marketing and Investor Attraction - Launch a comprehensive promotional campaign through social media and partnerships with blockchain companies. - Host meetings with investors to showcase progress and upcoming goals. - Duration: 2-3 months.

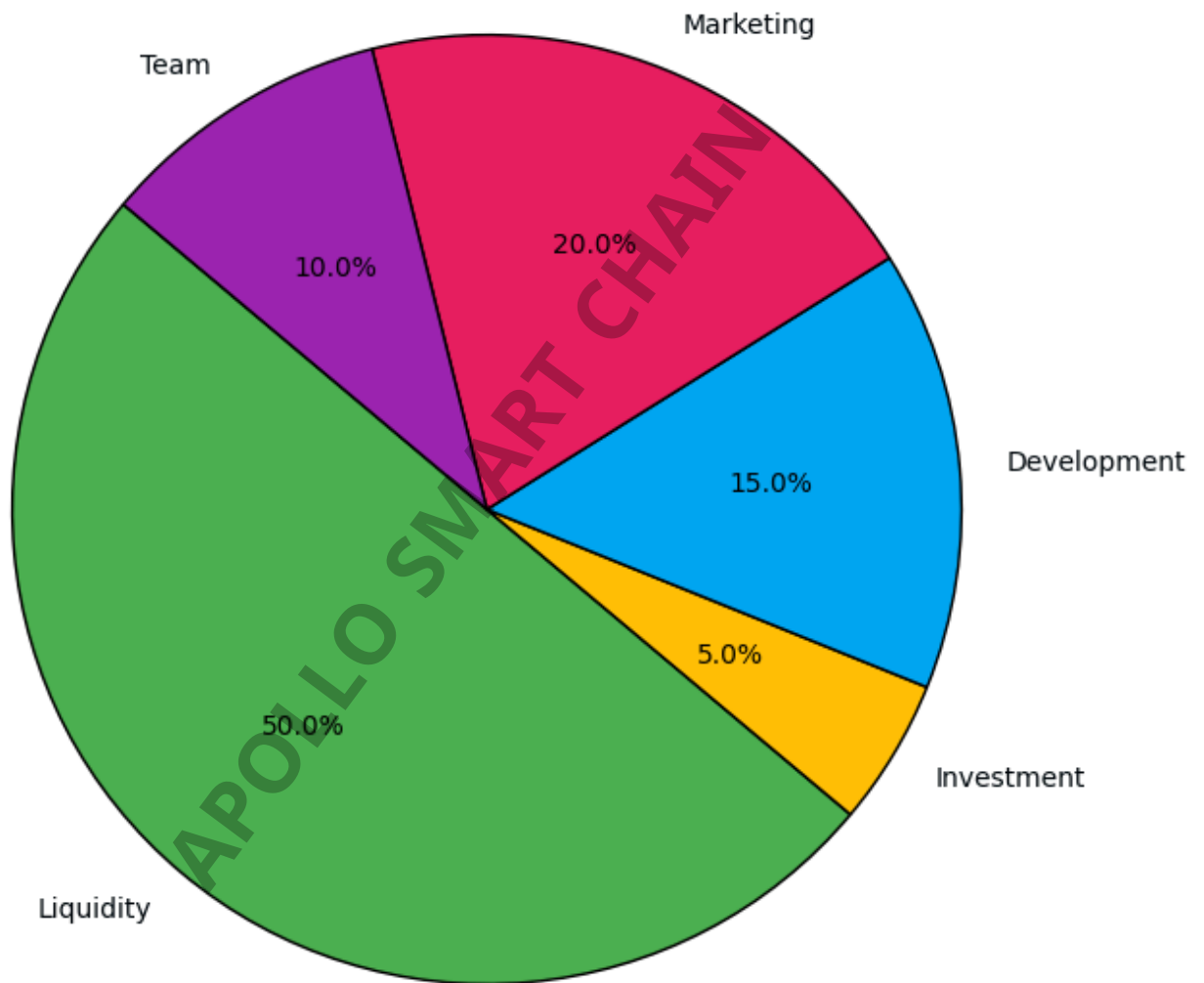
Q3 - Q4 of the Following Year (Month 19 - Month 24): Full Launch and Scaling

1. Full Launch and Feature Expansion - Launch the full version of all platforms, expand features to meet user needs. - Provide continuous security updates and advanced technical support. - Duration: 3 months. 2. AI Integration for Customer Assistance and Content Generation - Enhance AI to include interactive user support and automatic content generation. - Improve AI to generate images based on user preferences. - Duration: 1-2 months. 3. International Expansion and Market Growth - Enter new markets and increase partnerships with international exchanges. - Customize marketing campaigns for each local market and support regulatory requirements. - Duration: 2 months.

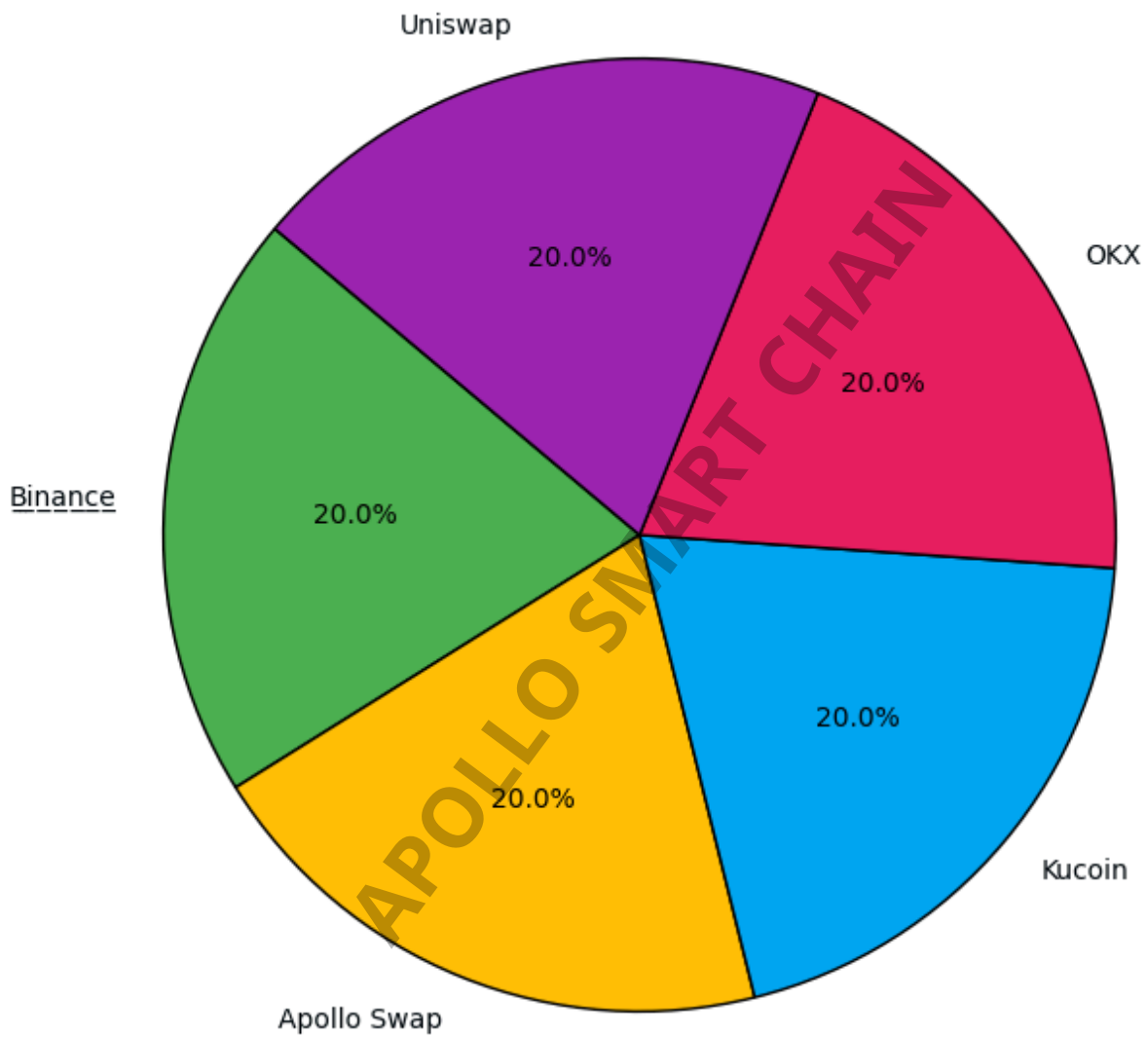
Alexander
Morgan

Apollo Smart Chain

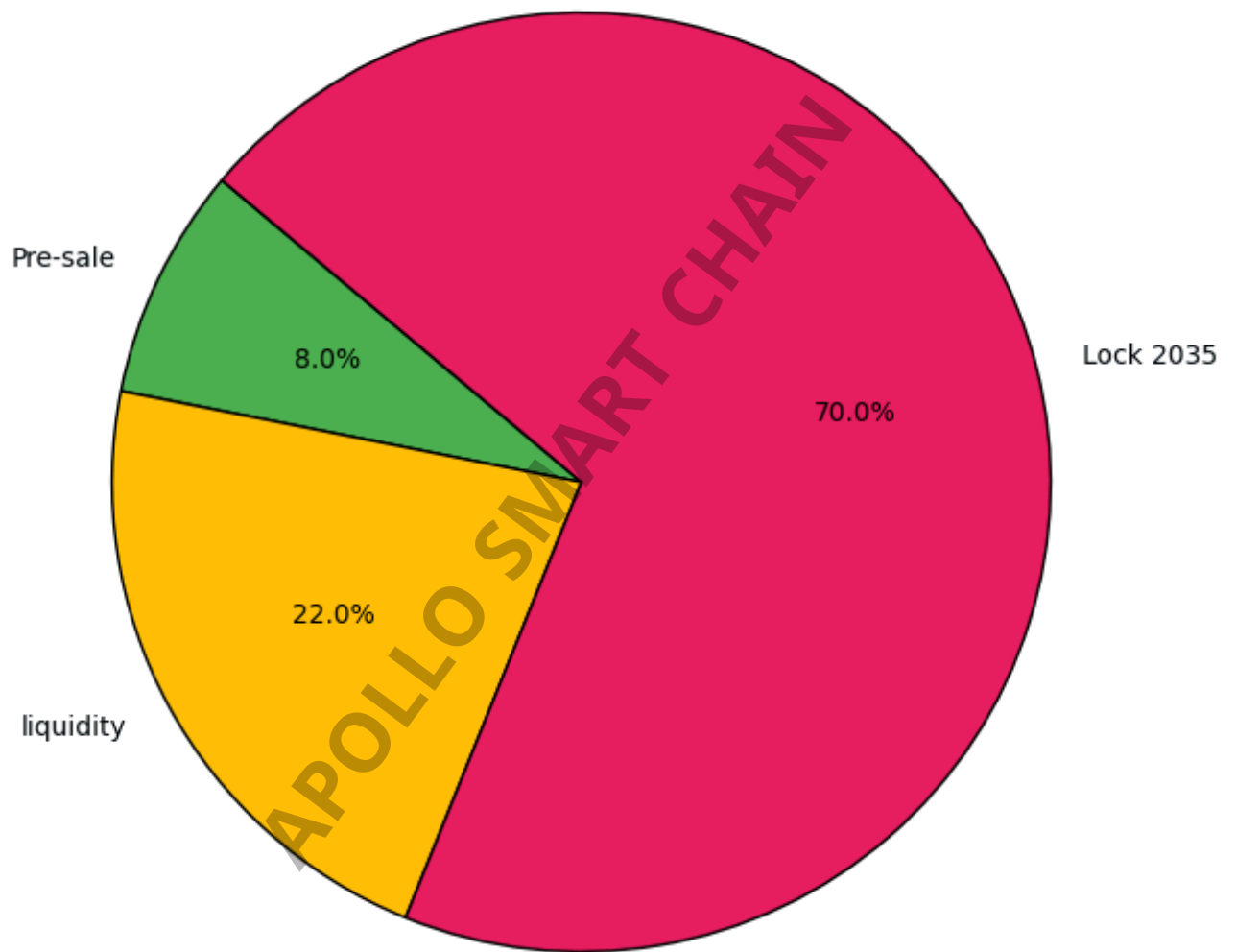
Token Allocation Distribution A S C



Token Allocation Distribution A S C



Token Allocation Distribution A S C



{#whitepaper}

Apollo Smart Chain

Alexander
Morgan



{#whitepaper}

<center>

<h1>ASCWhitepaper</h1>

</center>

< [Whitepaper Version 1]

Alexander Morgan <<

{#Abstract}

Abstract

Smart contract platforms and cryptocurrencies have captured mass attention but still have not been able to achieve mass adoption due to scalability and user experience issues. Even on Ethereum, which is the most widely used smart contracts platform, there have not been many examples of DApps which have seen mass adoption. There have been a few cases where one or the other particular application temporarily succeeded in achieving a significant user base, but it led to crippling of the entire network during the high network load times. Essentially this means that even the most advanced and widely used platforms are not ready for mass adoption yet.

On the other hand, there are a few smart contract platforms which boast of higher transaction throughput, but they compromise on decentralization in order to improve transaction speeds. Also, many of the upcoming solutions propose developing their own blockchains, neglecting the billions of dollars of market cap that DApps and other projects have already created on platforms like Ethereum and others. More importantly, they neglect the massive developer community and

developer ecosystem that currently exists on platforms like Ethereum.

ASCNetwork strives to solve the scalability and usability issues, while not compromising on decentralization and leveraging the existing developer community and ecosystem. It is an off/side chain scaling solution for existing platforms to provide scalability and superior user experience to DApps/user functionalities.

The ASCdevelopment team has chosen Ethereum as the first platform to showcase its scalability and already has a working implementation for Ethereum on Kovan Testnet. It is expected to allow near-instant transfers, exchange and conversion of digital assets (e.g. crypto tokens) and cryptocurrencies in the future. The ASCNetwork is an adapted implementation of the Plasma framework for Ethereum to start with, but the vision of the ASCdevelopment team is to provide off/side chain scaling solutions for blockchains in general. ASCfoundation intends to provide ASCwallet, payment APIs & SDKs, products, identity solutions and other enabling solutions that will allow developers to design, implement and migrate DApps built on base platforms like Ethereum. One of the key pillars that form the basis of ASCNetworks ideology is the improvement of user experience, this area is poorly developed for Blockchain applications as of now. The ASCDevelopment team has already built high quality user experience Mobile/Web browser libraries which will enable businesses to create real world end user applications on a large scale. The development roadmap of the ASCNetwork also includes supporting cross-chain transfers and third-party Decentralized exchanges, liquidity pools etc.

Why ASC?

Decentralized Apps are being proposed in large numbers, but the current blockchain ecosystem is not prepared to scale to match the demands of end user applications with mass adoption. Moreover the user experience of DApps is very poor and in no way conducive for average users. Slow block confirmations, high transaction fees, low scalability and poor user experience are some of the key roadblocks for the mass adoption of blockchain applications. The following section explains the

problems prevailing in the current blockchain ecosystem and how the ASCNetwork intends to solve them. **Detailed technical specification are provided in the further sections of the white paper.**

Slow Transactions {#slowt}

Blockchain transactions are typically very slow and have a very limited throughput. Most PoW ([Proof-of-Work])(based blockchain protocols have a limit on the block size and it takes a certain amount of time to generate a block. Each transaction also has to wait for multiple block confirmations due to potential chain re-organizations.

PoS ([Proof-of-Stake])(based blockchains try to counter these limitations using a staking mechanism, but the blockchains that are able to achieve high throughput with PoS are able to do so at the cost of decentralization. These limitations are often a necessary condition for public blockchains to ensure security and decentralization where a block needs to be propagated through the network and validated by all the nodes to achieve finality.

The ASCNetwork solves this problem by using a high throughput blockchain with consensus provided by a selected set of Block Producers, chosen for every checkpoint by a set of Stakers. It then uses a Proof Of Stake layer to **validate the blocks and publish periodic proofs (merkle roots) of the blocks produced by the Block Producers to the Ethereum mainchain. This helps in achieving high level of decentralization while maintaining an extremely fast (< 2 seconds) block confirmation times.**

Low Transaction Throughput {#ltht}

Public blockchains have to maintain a certain amount of time lag between the production of adjacent blocks so as to ensure ample time for block propagation. Also, the block size needs to be small so as to ensure quick propagation of the block through the network. This entails that the number of transactions in a particular block need to be fairly limited.

The ASCNetwork solves this problem by using a **Block Producer layer** to produce the blocks. Block Producers enable the system to produce blocks at a very fast rate. The system ensures decentralization using PoS checkpoints which are pushed to the Mainchain (Ethereum serves as the mainchain for a start). This enables The ASCNetwork to theoretically achieve up to 2^{16} transactions per second on a single side chain.

Scalability {#scalability}

As discussed in the previous section, The ASCNetwork easily achieves a theoretical speed of up to 2^{16} transactions per second on a single side chain. In future, The ASCNetwork is expected to be able to easily add more side chains horizontally to increase the total number of transactions on the ASCChain while using the same decentralized PoS layer.

Theoretically the ASCNetwork has the capacity for millions of transactions per second with the usage of multiple side chains. Also, the mechanism to do so has already been demonstrated with the first ASCproof-of-concept with the first ASCside-chain and new chains can be added in due course of time.

Size of Blockchain {#sob}

Each block on the blockchain and/or compute state in case of a smart contract based blockchain must be validated by multiple nodes. Each node has to manage a copy of the state and the blocks. While the chain increases in size as the days go by, maintaining and validating the whole blockchain becomes difficult and results in fewer full nodes in public blockchains, which poses a risk for decentralization.

For the ASCNetwork, the primary layer which provides decentralization may choose to store only the blocks of ASCChain from the previous checkpoint to the next checkpoint. All previous transaction/block proofs have been submitted to the mainchain. This enables extremely low fidelity PoS nodes which can be run in very low-cost machines with low storage. In future, The ASCNetwork

intends to enable mobile device based PoS miners too.**

Multiple micropayment channels with other off-chain solutions {#loooong}

Some payment channel solutions have proposed solutions to solve the problem of micro-payments. However, the process of opening and managing channels with multiple DApps or users is complex. Additionally, the speed and convenience of mediated payments over channels is still up for debate.

Since **The ASCNetwork uses a state-based architecture on an EVM (Ethereum Virtual Machine), it does not require payment channels to be opened between two parties. In fact, any valid Ethereum address is a valid ASCAddress and a receiver does not need to be on the ASCchain to receive payment. They would only need to have a ASCWallet when they want to retrieve the payments on the main chain or spend it in the ecosystem on the ASCNetwork.**

High Transaction Fees {#htf}

With the rapid growth of the blockchain ecosystem, new crypto assets are increasingly being created, transferred, and sold, often involving multiple crypto tokens. Also, most decentralized apps have their own token and economy. Paying tokens for the services or doing any kind of transaction on blockchains requires on-chain transfers. Every blockchain has a transaction cost structure. For example, Ethereum charges gas fees on each transaction.

The amount of fees is an important factor to incentivize validators and prevent certain kinds of security attacks such as DoS. However, there is the problem of variation of fees (Depending upon the pending transaction pool) due to the limited block size.

The ASCNetwork enables low cost transactions through achieving economies of scale by doing a large number of transactions on the Block Producer layer which ensures low cost, and then subsequently batching the proofs of the ASCblocks using the Merkle root of the blocks to a highly decentralized mainchain (for ex. Ethereum) using a decentralized layer of PoS Stakers.

Poor Usability {#pf}

User interactions on DApps are often poor compared to their centralized counterparts. For the Decentralization revolution to achieve mass adoption, the user experience of DApps has to be on par with, if not better than, their centralized counterparts.

The ASCDevelopment team is expected to work on various Mobile and Web browser integration tools and is pioneering protocols in this domain. It intends to build a ubiquitous mobile/browser app, which will act as a secured interaction layer for blockchain interactions. The ASCDevelopment team will be publishing the designs and prototypes of these soon.

Introducing the ASCNetwork {#imn}

As discussed in brief in the section above, the ASCNetwork aims to solve the problems faced by the blockchain ecosystem through building a decentralized platform using an adapted version of [Plasma](framework. This provides for fast and extremely low cost transactions with finality on a mainchain. The current working Testnet and alpha-Mainnet of the ASCNetwork works with Ethereum as a mainchain.

The ASCDevelopment team is also building a product ecosystem including user friendly mobile apps, desktop wallets and browser extensions which will provide a seamless experience for all users. It is envisaged that users will be able to pay, transfer or hold crypto assets without worrying about the complexity of the underlying system.

Architecture {#architecture}

Since the ASCNetwork's core focus is on mass user adoption, it is ideal that a deep dive into the ASCNetwork's technical architecture should start from a user journey.

When a user is transferring ETH or ERC20 tokens on the Ethereum network, they have to wait for the confirmation of the block which ranges from 14 seconds to 20 seconds. Even then the users

have to wait for multiple block confirmations to be sure of the finality of the transaction. Lets say you are buying a coffee or paying tokens to watch a movie. On each transaction you are not only paying a high fee, but also waiting for it to be confirmed. That serves as a deterrent for users wanting to use the service.

Moreover, during peak loads, a large number of transactions clog the Ethereum network and gas fees increase on each transaction in order to obtain faster confirmations. The ASCNetwork is proposed as a solution to overcome these problems.

Here is how the ASCNetwork will function:

1. A user deposits a cryptographic asset in the ASCcontract on the mainchain (currently implemented with Ethereum blockchain only).
2. Once deposited, tokens get confirmed on the main chain, tokens will appear on the ASCChain using ASCDeposit bridge (technical details explained in a dedicated section below).
3. The user can now transfer tokens to anyone they want almost instantly (ASCChain has faster blocks - approximately 1 second or less) for almost negligible fees.
4. Whenever the user wishes to, they can withdraw tokens to the main Ethereum chain by establishing proof of remaining tokens on Root contract (contract deployed on Ethereum chain).

The same method will work for any ERC-20 token or other fungible crypto assets on the Ethereum blockchain.

The ASCDevelopment Team has already created a demo version, available at

We expect the alpha version of the mainnet to go live very soon.

Actors {#actors}

The ecosystem of The ASCNetwork will have the following actors :

1. End Users

2. DApp developers : Developers are expected to use the ASCNetwork to scale their applications and provide a better UI/UX to their end users 3. Stakers : Stakers need to deposit/stake tokens to qualify and play a very important role in the ASCNetwork. They validate the transactions and propose checkpoints on the mainchain using PoS consensus mechanism with a majority. They also choose Block Producers amongst themselves, who satisfy a certain criteria, to produce blocks on the sidechains. 4. Block Producers : These are block producers chosen by Stakers who in turn enable faster blockchain generation times. They have to provide a significant stake to be nominated.

Consensus {#con}

The ASCNetwork uses a dual strategy of Proof of Stake at the checkpointing layer and Block Producers at the block producer layer to achieve faster blocktimes while ensuring a **high degree of decentralization by achieving finality on the main chains using the checkpoints and fraud proof mechanisms.**

Through this mechanism, The ASCNetwork achieves high transaction speed with a high degree of decentralization and finality on Mainchain. In the first version which has Ethereum only as the base chain, Ethereum root contract enforces solvency and finality through header block(checkpoints) very efficiently. The various elements and mechanisms of the system are described below:

Checkpointing Layer {#checklayer}

Basically, anyone can stake their ASCTokens on root contract to become a Staker in the PoS checkpointing layer (contract deployed on Ethereum chain). This provides a highly decentralized base layer for ASCChain.

Block Producers

At the blockchain layer of the ASCNetwork, there are Block Producers, selected by PoS Stakers on

the base layer, who will be creating the ASCBlocks. To achieve faster block generation times, these Block Producers will be low in number. **This layer is expected to achieve ~1 second block generation times at extremely low to negligible transaction fees.**

Checkpointing Mechanism

On ASCNetworks checkpointing layer, the basis of ASCNetwork's PoS mechanism, for every few blocks on the block layer of the ASCNetwork, a proposer will be chosen among the stakeholders to propose a checkpoint on the main chain. These checkpoints are created by the proposer after validating all the blocks on the block layer of the ASCNetwork and creating the Merkle tree of the block hashes since the last checkpoint. The Merkle root is then broadcasted to the Staker network for their signatures. The other stakeholders also verify the proof. They will approve the proposed block, if it is valid, by providing their signatures.

The system needs the approval of the stakeholders to propose a header block to the root contract. Once the checkpoint is proposed on the mainchain, anyone on the Ethereum mainchain can challenge the proposed checkpoint within a specified period of time. If no one challenges it and the challenge period ends, the checkpoint is formally included as a valid checkpoint on the main chain.

Apart from providing finality on the mainchain, Checkpoints have a very important role to play in withdrawals as they contain the proof-of-burn (withdrawal) of tokens in the event of user withdrawal. It enables the users to prove their remaining tokens on root contract using Patricia Merkle proof and header block proof. Note that to prove remaining tokens, the header block must be committed to the Root Chain through PoS (Stakeholders). The withdrawal process will incur Ethereum gas fees as usual.

Through this mechanism, The ASCNetwork achieves a high transaction speed, a high degree of decentralization and finality on Mainchain. In its first version which has Ethereum as the base chain,

the Ethereum root contract enforces solvency and finality through header blocks (checkpoints) very efficiently.

Block Producer Selection

Block Producers are chosen by Stakers in the checkpointing layer through voting on the mainchain. A Block Producer is selected for a pre-determined interval of time until slashed/removed by the network consensus mechanism or if it is unable to participate in the block production due to any external issue.

Seeding of the network

Block Producer application process

Selection through Voting at tenure completion

Replacement of a Block Producer during the ongoing tenure

In an event of untimely removal/incapability of a Block Producer to take part in block production, a new Block Producer from the transient pool will be recruited. An appropriate incentive mechanism to have a prioritized/preferred list of Block Producers as per the stakers' vote will be devised to maintain a healthy pool of Block Producers.

Multi Chain Support (Horizontal Sharding) {#multichain}

The ASCNetwork public checkpointing layer supports multiple side chains by design. Theoretically there can be an infinite number of side chains working under the secured and decentralized layer of checkpoints. Businesses can have their dedicated side chains connected to the public checkpointing layer having full control of their execution environments, while still retaining the immutability, provability and security of transactions via the checkpointing mechanism.

Key factors influencing design of this sharding process are expected to be:

1. Scheduling of checkpointing layer to periodically propose checkpoints for different side chains 2. Movement of assets across multiple side chains - User will be able to send assets across side chains using chain ids and receipts - Users will be provided with an intuitive wallet interface to perform inter-chain transactions - Developers will be provided with API/SDKs to build programmable interfaces for inter-chain transactions 3. Movement of the assets from one chain to another will be managed at the checkpointing layer and may not require any interaction with the mainchain. Research is currently underway to facilitate faster (possibly instant) inter sidechain transfers.

Interoperability {#interoper}

As mentioned earlier in the whitepaper, the Ethereum mainchain is the first base/mainchain that ASCNetwork securely integrates with, using an adapted implementation of the Plasma framework. In addition, the ASCnetwork intends to integrate multiple leading smart contract platforms cryptocurrencies such as Bitcoin and others to provide an universal platform for the users to be able to use/exchange their assets from various blockchains.

It can also provide a strong foundation for large DEXs (Decentralized exchanges) hosting assets from multiple blockchains. Also having a single platform with assets from multiple blockchains can also give rise to dramatically new use-cases, which the developer ecosystems can conceptualize their future products on. It is an exciting area of exploration for the ASCDevelopment team.

Judging from the proliferation of Layer 1 blockchains, it is a given that there might be more than 2-3 public blockchains that will be adopted by the mainstream eventually, rather than only a single winning blockchain platform. Therefore, the ASCDevelopment Team expects to see hitherto unseen use-cases, arising from the Decentralized application movement across these blockchains. The vision of the ASCDevelopment Team is to provide infrastructure and interfaces such that anyone who wishes to build decentralized applications on any blockchain, will be able to do it easily - and

communicate and transfer value across multiple blockchains.

Generalized State Scaling on Plasma {#genscaling}

Generalized State scaling is the next frontier for the ASCNetwork, once the ASCDevelopment Team is done with implementing micropayments, asset transfers and swaps in the first phase of development of the ASCNetwork. This is a research problem, and it will take time and effort to accomplish a breakthrough here.

There are mainly 3 different approaches that the team has been researching on:

- Stateful object programming model (separating code and state)
- State transition verification through zk-snarks
- State transition verification using an EVM-in-an-EVM construction

One of the main approaches that the ASCDevelopment Team has been researching on is the Stateful object programming model for Plasma. The main problem with applying the Plasma model to contracts on a sidechain is of the "ownership" of states/assets on the sidechain. One fundamental property of Plasma is that state represented on a Plasma chain must be able to be withdrawn to the root chain (e.g. Ethereum) in a way that maintains the integrity of that state. You should be able to freely move assets/state from the Plasma chain to the root chain, and vice versa. This functionality is particularly important when a consensus mechanism on the sidechain goes bad and users are forced to withdraw their assets/states from the Plasma chain.

States/assets belonging to a user (Externally Owned Accounts) are easy to deposit/enter and withdraw/exit from the mainchain to the sidechain and vice versa. However, in terms of contracts, it is not easy to identify the ownership of the state - because the state might be owned/controlled by multiple parties. The most promising approach to solving this problem is basically separating state and code.

What this approach entails is to enable writing code which reads/writes into "stateful" objects. Stateful objects are representation of states which have a clear owner. For example, a contract has a set of states controlled by n parties, then stateful objects will be derived by encapsulating state into non-fungible tokens having clear ownership - this way a stateful programming model is introduced that enables these objects to be exitable and therefore Plasma-ficable.

The second approach entails the usage of zk-snarks for verifying state transitions for a sidechain. Basically one could operate a [roll-up](style chain, which can perform any state transitions, and a zk-proof can be submitted.

A valid state transition is proven within the snark by opening one or several leaves of the describing the current state, checking the users signatures, doing predefined operations, updating the leaf and finally recalculating the stateRootHash. DApp-specific roll-up style chains on the plasma chain can allow developers to have secure, high-throughput DApps without worrying about liveness, data-availability issues or withdraw issues. We can store any information we want in leaves of the trees and write the snark logic on how they should be updated, since invalid snark proofs cannot be pushed and so it's inherently secure and simple. We are actively researching on this area and trying to come up with a secure and scalable construction.

The third approach involves a Plasma sidechain implementation that can run EVM-compatible smart contracts - i.e. the ASCVirtual Machine. Since the philosophy of the ASCNetwork heavily revolves around an incentive mechanism of security deposits on the main chain, it can be instructive to think about an efficient way of identifying the data involved in fraud challenges.

Validation of consensus rules can be enforced through a system of challenges, using a [TrueBit](verification. The main motivation is to run software in a similar manner as we currently do on the Ethereum mainchain. The security deposit makes it easier to estimate the security of the sidechain in monetary terms. When working correctly, the stakers will frequently commit the sidechain blocks to the root chain.

A set of validations is expected to keep the stakers honest. There are a number of insurance contracts incentivizing the verification of the chain. Together these contracts combined would make for a complete set of consensus validation rules on the root blockchain. Such rules include:

- Withholding challenges: The Block Producers might have submitted blocks to the blockchain but have withheld the contents. The stakers must present a preimage or risk getting slashed.
- Parsing challenges: The Block Producers submitted an invalid block structure.
- Transaction censorship: Submit a transaction on the root chain, requesting for it to be included in the sidechain within a certain timeframe.
- Invalid block signature: The stakers provided an invalid signature of the block.
- Invalid previous block hash, height, or previous state, among other block verifications.
- Any other consensus failure checks, like transaction receipts posting an invalid after state.
- Invalid transaction execution: an on-chain way to verify a transaction.

The last step is the most complex technically, but using a Truebit-like binary search, there would only be a need to verify one EVM state transition.

A precompile is required to run the EVM inside an EVM. This is done through a stepper contract that can compute a EVM state transition.

Some work on this already started (see [solevm]) but the focus will be to correctly encode the whole EVM state in such a way that it can fit inside a transaction in the root chain, for the purposes of verifying it with an interactive Truebit game. The ASCDevelopment Team believes that a large security deposit, plus other economic interests that participants might have in the correct operation of the sidechain, would lead to less risks.

Overall, if one can efficiently identify the problem EVM state transition for verification, through an EVM-in-an-EVM construction, one can subject it to challenges, and thereby securing it.

Security

Fraud Proofs {#fraud}

To enhance the security of the transactions, ASCNetwork also provides Fraud Proofs on the mainchain. The mechanism enables any individual on the mainchain to submit the details of the transactions which he/she thinks is fraudulent. If the challenge is successful, the stakes of the parties involved in the fraud are slashed and the challenger receives the slashed funds as an incentive for detecting the fraud. This can be considered as an always-running high reward bounty program for any parties who wish to investigate the veracity of the transactions on the ASCNetwork.

Basic proofs {#basicp}

Each proof must be submitted with the following corresponding proofs whenever necessary:

- Merkle proof for transaction inclusion: This type of proof is needed to prove that the given transaction is included in the block
- Merkle proof for block inclusion: This type of proof is needed to prove that the block is included in the given checkpoint

Block {#blockp}

This proof is needed to prove that the block is in sequence with a valid referenced hash.

Transaction

Single level txn proof {#singletp}

Nonce validation {#noncevp}

- To check if there are transactions with duplicate nonces
- To check for transactions with missing nonce values (skipping multiple nonces in between)

This is an interactive fraud proof. The Block Producer must submit missing nonce transaction in

certain amount of time when challenged for this type of transaction.

- To check for transactions with non-ordered nonces

Receipt validation {#recvalp}

- To check receipt fields, events, topics and data types in given receipt

Deposit {#depositp}

- Validate deposit transactions

Validates deposit transaction on the mainchain and see if it matches with DepositBlock object in rootchain.

- Duplicate deposit transactions

This proof validates if there are duplicate transactions that have the same DepositId and that each DepositID is included only once

- Validate deposited amount and the depositor address

ERC20 transfer {#erc20tp}

- To validate ERC20 transaction data, receipt logs and values
- To check if UTXO-style input in log receipt log equals that of an UTXO-style output of a recent transaction log receipt

Iterative txn proof

Details to be updated in a later version of the whitepaper

Network Economics {#economics}

Transaction Fee Determinative Factors and Trade-off

1. Block Size = (Average Transaction Amount)/(Block)

- 100Txs/Block is insanely expensive.
- ETH is 600~1000Txs/Block
- If The ASCNetwork permits 3000Txs/Block, this variable is going to be the predominant factor over other factors.

2. Number of Block Producers

- If there are more Block Producers, transaction fee allocation will be more.
- Block Producer setting of 7 is cost efficient.
- If the number of Block Producers is increased to say, 120, the transaction fee increases.

3. Number of Checkpoint stakers

- If number of stakers is 10,000, then it will be expensive to structure incentives.
- 100-150 stakers will result in an optimum transaction fee.
- Having fewer stakers than this is better, but decentralization in such a setup is lower.

4. Block Time

- The ASCDevelopment team could assign 2~3sec for block time.
- 0.5sec block time still works with regards to block propagation, and it has no effect on user experience.
- Let's say, a single ASCsidechain aims to achieve ~35k Tx/sec on a chain. If node through-put is the bottleneck, then blocksize would be 70k~105k Tx/Block.

5. Checkpoint duration - A checkpoint duration of ~300sec (256 blocks on sidechain) has been determined to be optimum. - A shorter duration means faster Maliciousness detection, but it also means a higher committed Gas fee. - If a Byzantine behavior (e.g. Double Spend through Tx deletion) occurs just after checkpoint creation, this duration is the worst-case time until the Ceremony. If some Block Producers delete

transactions, the ASCNetwork can recover the cancelled transaction, and the double spend attack would be foiled.

Focus on User Experience {#usere}

The ASCDevelopment Team is developing a wallet by implementing the [WalletConnect](protocol, which is an open protocol to connect web-based distributed applications to mobile crypto assets.

This wallet will help users to interact with DApps and sign transactions easily, while still helping users keep their private keys safe on their mobile. This should go a long way in making blockchains accessible to mainstream users.

Other than this, the team is also looking at context specific ether-less accounts and Gas relay abstraction on identity to enable ether-less sign transactions, which can be a huge boost for mainstream user adoption.

ASCStack {#stack}

This section details out various parts of the ASCchain and components in the Ethereum chain.

ASCcontracts on mainchain {#mcontracts}

The ASCsmart contracts on the mainchain provide the core logic for the ASCNetwork. The contracts contain various mechanisms such as deposit and exits from the mainchain to the sidechain and vice versa. They also contain the exit priority queue, the periodic state commitments from the Validator layer, fraud proof mechanisms, bonded exit challenge logic and various other components. The Stake Manager also resides here.

ASCDeposit Bridge {#mdb}

The bridge(s) of the ASCNetwork are part of Block Producer nodes that listen to the RootContract events on the mainchain and monitor any token/ether transfer events happening to the

RootContract. This bridge utilizes ASCNetworks famous tool named . Once the bridge detects a deposit on the mainchain, it fires a Deposit event on the ASCchain and the users address on the ASCNetwork is allocated the deposited amount.

ASCPoS {#mpos}

The checkpointing mechanism of the ASCNetwork is a PoS enabled layer which has Stakers who propose the checkpoints to the mainchain. There will be about 100-150 Stakers at the checkpointing layer to start with. In future with the advent of more efficient signature mechanisms on the Ethereum blockchain, the ASCNetwork will be able to significantly increase its number of stakers on the checkpointing layer which is expected to further increase its degree of decentralization, perhaps rivalling that of the leading public blockchains like Ethereum and Bitcoin.

More details of the PoS checkpoint layers will be given in a later version of the Whitepaper.

Block Producer Layer {#bplay}

At the base layer, the ASCNetwork has Block Producer nodes chosen by the Stakers of the PoS layer through voting for every checkpointing interval. These Block Producers will also run the ASCDeposit bridge.

Block Producers accept transactions through the ASCVM and are expected to create a block every ~1 second.

More technical and code level details of the Block Producer layer will be added in a later version of the whitepaper.

ASCVirtual Machine {#vm}

The ASCNetwork uses a standard EVM based state machine, which is run by the Block Producer nodes to generate blocks. Using the EVM allows the ASCNetwork to be able to build and deploy

protocols such as ERC protocols as well as other protocols like Kyber Network, ZRX etc.

The beauty of the ASCNetwork architecture is that since it uses an EVM-compatible state machine, it becomes very easy to port DApps and smart contracts running on the Ethereum blockchain to the ASCNetwork. The ASCDevelopment Team intends to support generalized state transitions on the ASCNetwork, and this architecture provides a smooth foundation to build upon.

ASCWithdrawal Bridge {#mvp}

When an address on the ASCNetwork submits a withdrawal request to the network, the corresponding tokens are burnt (withdrawn from) on the ASCchain and this transaction is pushed on to the ASCchain. After the specified checkpoint interval, the PoS checkpoint layer will publish the checkpoint to the main chain, which will include the proof of burn (withdrawal) of these tokens on the ASCchain. Once this checkpoint is committed on the mainchain, the user can claim their withdrawn tokens.

Spam Protection {#spam}

The Block Producers running the block producer layer of the ASCNetwork will watch the transfer state of the assets to identify frivolous transactions. They reject any incoming transactions with zero amount in payments thereby foiling any DoS/spam attacks with zero cost transactions. Even if the ASCtokens are very low in cost and the fees being very low, due to the high TPS of ASCNetwork, it would not be economically viable to run sustained DoS attacks on the ASCNetwork.

The ASCNetwork maintains payment transfer event logs in a UTXO-like data structure, which allows for efficient verification of inputs and outputs. This allows for a variety of security measures.

Additional checks are run to mitigate spam based on this:

- For each input, the referenced output must exist and cannot already be spent
- Check if the sum of input values is less than sum of output values.

- Check if transaction fee is too low.
- Check for duplicate transactions with same outputs in the transaction pool.
- Check for duplicate transactions with same transaction fee in the pool.

Potential Use Cases {#potential}

ASCNetwork Pte. Ltd. (The Governing body) is committed to provide a scalable and user- friendly ecosystem for third party Decentralized applications to thrive on. The governing body, like Ethereum and other platform foundations, will promote various Base chain DApps (like DApps built on Ethereum currently, and NEO, EOS in future) to build and migrate their user facing applications / transactions on the ASCNetwork. It will also award grants and funding to third party app developers to build various use cases on top of the ASCNetwork like:

Payments {#payment}

The ASCNetwork will provide an interface for users, payment APIs and SDKs for DApps, merchant and users to instantly accept or pay in crypto assets (e.g., ERC20 tokens, Ethers, ERC721 tokens).

The ASCDevelopment Team has plans to roll-out this system in three phases:

1. Ether and ERC20 token payments
2. Multi-asset cross chain transfer and payment through atomic swaps and liquidity providers
3. Fiat enabled off-ramp payment system integration through fiat liquidity providers

Atomic Swaps {#atom}

ASCcontract allows users to pay with any crypto token they prefer, and receiver will receive payment in assets they prefer. The ASCNetwork can handle conversation through atomic swaps between cross-chain crypto assets.

Liquidity providers {#liquidity}

Third parties can use the ASCNetwork to exchange any tokens for other tokens by leveraging 0x liquidity pool or other liquidity providers while transferring crypto assets. In the case of fiat, the ASCDevelopment Team is planning to collaborate with fiat liquidity providers in currencies of major countries.

Decentralized Exchange (DEX) and Marketplace support {#dex}

The ASCNetwork is expected to have all characteristics which an exchange platform should have faster and cheaper trades. The ASCNetwork is capable of supporting decentralized exchanges and enabling trust-less, reliable and easy crypto trades. The decentralized exchange is the future for digital assets and provides better security and solvency than the centralized exchanges.

Lending & Credit Scoring platform {#lcsp}

The ASCNetwork will enable platforms for merchants to assess the creditworthiness of connected users via their transaction history. This enables merchants to lend tokens to users on the network when transacting with users that do not have sufficient funds. The ASCNetwork expects to use the Dharma protocol to provide tokenized debt to users.

Identity {#identity}

Users need a utilitarian yet user-friendly interface where MetaMask or web3 enabled browsers are not required. They do not need to understand how Ethereum works under the hood.

Decentralized apps need a way to sign transactions, but that must happen without submitting private keys on each DApp on web browsers or mobile apps. The ASCDevelopment Team believes that users must have control over their private keys without worrying about the security. The ASCNetwork will solve that with an Open-Identity system and will deliver a seamless experience to users.

This system will also provide a way to auto-approve certain kind of transactions depending upon the

criteria chosen by the users. This will drive the recurring payments on the ASCNetwork.

Games {#games}

We expect games to be a big part of the ASCNetwork. In-game assets represented as NFTs (ERC721) are expected to be bought, sold and traded in huge numbers on our sidechains. Developers will also be able to save game state on the sidechains, if they choose to. Along with the NFT marketplace that we will enable, developers and users will truly have a fast, efficient and secure sidechain to build and play games on.

Infrastructure {#infrastructure}

The ASCDevelopment Team will act on the simple mantra - make it simple and seamless. For that, the team will provide new infrastructure around the ASCNetwork including user-friendly wallets for individual users and merchants, payroll dashboards, payment SDKs and other open source tools.

Dagger {#dagger}

The ASCDevelopment Team already has started building infrastructure for developers, starting with Dagger. [Dagger](is a tool or engine to track Ethereum accounts and events in real-time.

Developers can use Dagger to track their own smart contracts, accounts, and transactions. They can create custom service or integrate with third-party services through IFTTT or Zapier.

ASCWallet {#mwallet}

The ASCdevelopment team is working on building an easy-to-use Plasma wallet mobile app, integrated with WalletConnect, to ensure secure storage of keys, intuitive access to the features provided by the ASCNetwork, as well as a seamless mechanism to connect browser-based DApps to the mobile app. Users can interact with DApps on browsers and in the future many more devices, while still keeping their keys secure in their mobile wallet.

The ASCwallet will act as a ready tool for DApp developers to get their users onboarded and working with ASCsidechains quickly and efficiently.

ASCTokens

The native digital cryptographically-secured utility token of the ASCNetwork (ASCToken) is a major component of the ecosystem on the ASCNetwork, and is designed to be adopted for use as the primary token on the network. ASCToken will be issued as ERC-20 standard compliant digital tokens on the Ethereum blockchain.

ASCToken is designed to be a utility token which functions as the unit of payment and settlement between participants who interact within the ecosystem on the ASCNetwork. ASCToken does not in any way represent any shareholding, participation, right, title, or interest in the Governing body, the Issuer, its affiliates, or any other company, enterprise or undertaking, nor will ASCToken entitle token holders to any promise of fees, dividends, revenue, profits or investment returns, and are not intended to constitute securities in Singapore or any relevant jurisdiction. Ownership of ASCToken carries no rights, express or implied, other than that which may be afforded by the ASCNetwork and/or any other third parties whom may use such Tokens.

ASCTokens are expected to provide the economic incentives to encourage participants to contribute and maintain the ecosystem on the ASCNetwork. Computational resources are required for performing various functions on the ASCNetwork such as validating blocks and publishing proofs, thus providers of these services / resources would be rewarded with ASCtokens for providing these resources to the network (i.e. "mining" on the ASCNetwork) to maintain network integrity. ASCToken will be used as the unit of exchange to quantify and pay the costs of the consumed computational resources. ASCToken is an integral and indispensable part of the ASCNetwork, because without the ASCToken, there would be no incentive for users to expend resources to participate in activities or provide services for the benefit of the entire ecosystem on the ASCNetwork. Only users which have actually contributed to network maintenance would receive token incentives. Users of the

ASCNetwork and/or holders of ASCToken which did not actively participate will not receive any ASCToken as rewards.

In order to participate in the consensus process on the ASCNetwork, users would be required to stake ASCToken as an indication of that user's commitment to the process. ASCToken would thus also be used as a deterrent for punishing stakers for various offences (e.g. invalid blocks, illegally verifying blocks, or invalid transaction execution) by requiring them to first put up a stake of ASCToken before being entitled to participate in the ecosystem. ASCToken would be deducted in the event that an offence was committed by a staker.

In particular, it is highlighted that ASCToken:
 1. is non-refundable and cannot be exchanged for cash (or its equivalent value in any other virtual currency) or any payment obligation by the Governing body, the Issuer or any affiliate; 2. does not represent or confer on the token holder any right of any form with respect to the Governing body, the Issuer (or any of its affiliates), or its revenues or assets, including without limitation any right to receive future dividends, revenue, shares, ownership right or stake, share or security, any voting, distribution, redemption, liquidation, proprietary (including all forms of intellectual property or licence rights), or other financial or legal rights or equivalent rights, or intellectual property rights or any other form of participation in or relating to the ASCNetwork, the Governing body, the Issuer and/or their service providers; 3. is not intended to represent any rights under a contract for differences or under any other contract the purpose or pretended purpose of which is to secure a profit or avoid a loss; 4. is not intended to be a representation of money (including electronic money), security, commodity, bond, debt instrument or any other kind of financial instrument or investment; 5. is not a loan to the Governing body, the Issuer or any of its affiliates, is not intended to represent a debt owed by the Governing body, the Issuer or any of its affiliates, and there is no expectation of profit; and 6. does not provide the token holder with any ownership or other interest in the Governing body, the

Issuer or any of its affiliates.

The contributions in the token sale will be held by the Issuer(or its affiliate) after the token sale, and contributors will have no economic or legal right over or beneficial interest in these contributions or the assets of that entity after the token sale. To the extent a secondary market or exchange for trading ASCToken does develop, it would be run and operated wholly independently of the Governing body, the Issuer, the sale of ASCToken and the ASCNetwork. Neither the Governing body nor the Issuer will create such secondary markets nor will either entity act as an exchange for ASCToken.

Features on our development roadmap {#future}

The ASCDevelopment team expects to conduct various additional research based on topics proposed by the community, including but not limited to:

1. Generalized state scaling and fraud proofs/cryptographic mechanisms for the same.
2. Evaluate the approach to expand Staker base in the checkpointing layer with the future Threshold based signatures implementations on Ethereum, if any.
3. Robust structure and design pattern for upgradeable smart contracts.
4. Context specific Ether less accounts and Gas Relay Abstractions on Identity
5. Privacy-enabled transactions
6. Blockchain interoperability
7. State channels on top of the sidechain

Risks {#risks}

You acknowledge and agree that there are numerous risks associated with purchasing ASCToken, holding ASCToken, and using ASCToken for participation in the ASCNetwork. In the worst scenario, this could lead to the loss of all or part of the ASCToken which had been purchased. IF YOU DECIDE TO PURCHASE ASCToken, YOU EXPRESSLY ACKNOWLEDGE, ACCEPT AND

ASSUME THE FOLLOWING RISKS:

1. Uncertain Regulations and Enforcement Actions : The regulatory status of ASCToken and distributed ledger technology is unclear or unsettled in many jurisdictions. The regulation of virtual currencies has become a primary target of regulation in all major countries in the world. It is impossible to predict how, when or whether regulatory agencies may apply existing regulations or create new regulations with respect to such technology and its applications, including ASCToken and/or the ASCNetwork. Regulatory actions could negatively impact ASCToken and/or the ASCNetwork in various ways. The Foundation, the Distributor (or its affiliates) may cease operations in a jurisdiction in the event that regulatory actions, or changes to law or regulation, make it illegal to operate in such jurisdiction, or commercially undesirable to obtain the necessary regulatory approval(s) to operate in such jurisdiction. After consulting with a wide range of legal advisors and continuous analysis of the development and legal structure of virtual currencies, a cautious approach will be applied towards the sale of ASCToken. Therefore, for the token sale, the sale strategy may be constantly adjusted in order to avoid relevant legal risks as much as possible. For the token sale, the Foundation and the Distributor are working with Tzedek Law LLC, a boutique corporate law firm in Singapore with a good reputation in the blockchain space.

2. Inadequate disclosure of information : As at the date hereof, the ASCNetwork is still under development and its design concepts, consensus mechanisms, algorithms, codes, and other technical details and parameters may be constantly and frequently updated and changed. Although this white paper contains the most current information relating to the ASCNetwork, it is not absolutely complete and may still be adjusted and updated by the ASCDevelopment team from time to time. The ASCDevelopment team has no ability and obligation to keep holders of ASCToken informed of every detail (including development progress and expected milestones) regarding the project to develop the ASCNetwork, hence insufficient information disclosure is inevitable and reasonable.

3. Competitors : Various types of decentralised applications are emerging at a rapid rate, and the industry is increasingly competitive. It is possible that alternative networks could be established that utilise the same or similar code and protocol underlying ASCToken and/or the ASCNetwork and attempt to re-create similar facilities. The ASCNetwork may be required to compete with these alternative networks, which could negatively impact ASCToken and/or the ASCNetwork.

4. Failure to develop : There is the risk that the development of the ASCNetwork will not be executed or implemented as planned, for a variety of reasons, including without limitation the event of a decline in the prices of any digital asset, virtual currency or ASCToken, unforeseen technical difficulties, and shortage of development funds for activities.

5. Security weaknesses : Hackers or other malicious groups or organisations may attempt to interfere with ASCToken and/or the ASCNetwork in a variety of ways, including, but not limited to, malware attacks, denial of service attacks, consensus-based attacks, Sybil attacks, smurfing and spoofing. Furthermore, there is a risk that a third party or a member of the Foundation, the Distributor or its affiliates may intentionally or unintentionally introduce weaknesses into the core infrastructure of ASCToken and/or the ASCNetwork, which could negatively affect ASCToken and/or the ASCNetwork. Further, the future of cryptography and security innovations are highly unpredictable and advances in cryptography, or technical advances (including without limitation development of quantum computing), could present unknown risks to ASCToken and/or the ASCNetwork by rendering ineffective the cryptographic consensus mechanism that underpins that blockchain protocol.

6. Other risks : In addition, the potential risks briefly mentioned above are not exhaustive and there are other risks (as more particularly set out in the Terms and Conditions) associated with your purchase, holding and use of ASCToken, including those that the Foundation or the Distributor cannot anticipate. Such risks may further materialise as unanticipated variations or combinations of the aforementioned risks. You should conduct full due diligence on the Foundation, the Distributor,

its affiliates and the ASCDevelopment team, as well as understand the overall framework, mission and vision for the ASCNetwork prior to purchasing ASCToken.

{#whitepaper}

Apollo Smart Chain

*Alexander
Morgan*

