ADN

WHITEPAPER VERSION 1.0

1. Introduction

Bitcoin will always be one of the most innovative developments in the history of money. Bitcoin, as the first decentralized digital asset, proved that it is possible for something intangible, with no issuer and no backing, to have a trillion-dollar market. The popularity of Bitcoin as a payment network and a new kind of money not only attracted fintech pundits, but also traders and investors looking to exchange fiat money to digital assets in hopes of making a profit as prices advance. Because of the demand for digital assets, Bitcoin's existing concepts had been used as a reference to develop more cryptocurrencies that contributed to the creation of many marketplaces that allow trading in digital currencies. Projects like ETH, EOS, and TRON are also major contributors in the expansion of the cryptocurrency space. By enabling developers to create their own coins through a main network (mainnet), these projects are responsible for paving the way for new cryptocurrencies to emerge.

Although cryptocurrency's technical contributions are truly innovative and beneficial, there are many negative aspects that arose due to an existing gap in the cryptocurrency industry; the lack of Initial Coin Offerings (ICOs).

Ever since the first token sale by Mastercoin in July 2013, many ICOs followed. One of the most notable ICO is Ethereum's ICO that raised 3700 BTC (approximately $2.3 million during that time) in the first 12 hours. More and more ICOs report success in raising funds, but now more than ever, cryptocurrency investors know that it's not all positive since it has caused financial loss as well.

Despite having successful ICOs, it has been criticized as a mechanism used to commit fraud. There are many investors who became victims to scammers who are applying a "pump and dump" scheme in which the scammers boost their ICO through marketing and promises of future profit, and then cashes out by dumping the coin. In this situation, investors are left to suffer with huge financial losses.

1.1 Vision

What ADN intends to provide is a blockchain with high-throughput, high scalability, and high availability for Decentralized Applications (DApps) in the ADN ecosystem. Combining the benefits initially proposed by its cryptocurrency predecessors such as Bitcoin, Ethereum, EOS and TRON, The project will also have a built-in investor-oriented mechanism programmed to protect the interests of the investors when they invest in cryptocurrency projects ICOs based in ADN.

1.2 Background

Contrary to popular opinion, the concept of decentralized digital currency has been floating around for decades. In the 1980s, individuals and organizations used Chaumian blinding to make private — if not entirely anonymous — transactions. However, the initiative failed because the protocol relied on a centralized intermediary. Another precursor to cryptocurrencies is B-money which is claimed as an “anonymous, distributed electronic cash system.” The idea was able to turn the heads of people, yet it failed to gain traction because its proponent, Wei Dai, couldn’t provide a detailed and tangible explanation on how decentralized consensus could be done.

It was only during 2009 when an unspecified figure who went by the name Satoshi Nakamoto demonstrated what his predecessors failed to accomplish. He was able to make a digital transaction by using a digital and decentralized currency, which we now know as Bitcoin.

1.3 Introduction of Existing Concepts

1.3.1 Bitcoin

Bitcoin uses Proof-of-Work (PoW), a consensus algorithm that solves the needs of cryptography while attaining the lofty ideal of decentralization. The algorithm allows anyone to join its network, thereby promoting decentralization and giving users the power to defend the network from Sybil attacks. This is accomplished by replacing a formal barrier to an economic barrier, wherein a node that has more computing power will have more weight in the consensus voting process.

1.3.2 Ethereum

Ethereum created a protocol that is focused on building decentralized applications and providing a platform for different tradeoffs to occur. It highlights high-speed transactions and development, security, and interoperability among its users.

Ethereum made this possible by building a blockchain network with a built-in Turing-complete programming language which allows anyone to write Smart Contracts and develop Decentralized Applications (DApps). This platform gives the users freedom to create their own rules for ownership, transaction formats and state transition functions.

The structure behind Ethereum is intended to follow the principles of simplicity, universality, modularity, agility, and non-discrimination and non-censorship.

The Ethereum protocol is crafted to be as simple as possible. An average programmer or developer should be able to implement the entire specifications of the network, as to create a democratic and original platform that will bring cryptocurrencies together. Any upgrade which adds complexity should not be included unless that enhancement would provide a significant benefit to all.

A vital part of Ethereum's design philosophy is that it is not bounded with rigid features. Anything is possible with Ethereum in your hands - digital assets, operating systems, and maintaining databases, among other functionalities.

Over the course of development, Ethereum's goal is to remain basic and operational as possible. It is a program where if one was to make minimal changes in one aspect, the application in general would continue to function without any discrepancies.

The details which the Ethereum protocol is working upon are not fixed. Although it needs a comprehensive analysis before making alterations, once results show that certain modifications are needed to improve scalability or security, the Ethereum Virtual Machine (EVM) might be upgraded.

The Ethereum protocol is constructed to avoid restrictions or preventive measures in specific categories of usage. All mechanisms are merely regulators for possible risks, but it does not attempt to oppose undesirable applications.

1.3.3 EOS

Since the introduction of blockchain technology in 2008, entrepreneurs and developers have strived to incorporate the technology in a wider range of applications on a single blockchain network.

EOS has designed a blockchain architecture that has the potential to scale by enhancing its transaction-per-second (TPS) performance, reducing latency to 1.5 seconds, removing per-transaction fees, and offering a better user experience than those provided by prevailing centralized services.

Applications on the EOS blockchain is adaptable enough to support millions of users, offer free services, develop new upgrades, resolve bugs, avoid delayed responses, handle high volumes of transactions, and could simultaneously function in different settings.

In some circumstances, a blockchain application needs a certain number of users for it to work in its optimum performance. For this to be easily done, a platform should be able to handle a huge number of users to ensure the best user experience.

Blockchain-based applications should be regularly updated for an enhanced user experience. The platform supports software and smart contract upgrades, thus developing new features, resolving bugs, and fixing other problems that might have been reported. A well-developed and stable platform could be modified without causing any delays and must be robust enough to recover from any unexpected failures or sudden errors.

Ensuring that a response will be given in a matter of seconds will make applications built on a blockchain stand out and outperform applications which are under a centralized, controlled system. The EOS platform supports low latency in transferring data and real-time transactions.

A platform should be able to simultaneously function across different settings. EOS' interoperability works perfectly, which then results in high-performance transactions performed successfully.

1.3.4 TRON

The Great Recession of 2007-2008 allowed individuals to recognize the changes that the banking and finance sector needs in order to adjust to the needs of the people. The birth and immediate fame of Bitcoin proved this to be true. From having a worth of virtually nothing, Bitcoin has become one of the most expensive commodities. It peaked in 2017, valuing around $20,000 USD which was largely due to the promise of providing smart, secure, decentralized, and anonymous transactions using blockchain technology, specifically through the Proof-of-Work (PoW) consensus mechanism.

Six years later, Ethereum was officially launched to allow developers to create their own Decentralized Applications (DApps) through what we now know as "smart contracts". But both Bitcoin and Ethereum encountered one adamant stumbling block which hindered their way to mass adoption: scalability. As more people used these cryptos for day-to-day transactions, throughput times slowed down, while fees increased. People had to turn elsewhere, or, as in the case of the crypto community, create a new technology that can be relied on. Hence, TRON was created to solve the scalability issues which haunted Bitcoin and Ethereum.

2. Architecture

The ADN protocol is designed to become a high-performance blockchain platform wherein developers can create DApps. It focuses on protecting the investment of ICO participants through its investment protection mechanism. These will be further elucidated below.

2.1 ERC-20 Token

ADN will start off as an ERC-20 token — it will be developed on the Ethereum blockchain.

ERC-20 tokens are tokens designed and used solely on the Ethereum platform. They follow a list of standards so that they can be shared, exchanged for other tokens, or transferred to a crypto-wallet.

There are six unique functions that ERC-20 expounds for the sake of other tokens within the Ethereum network. These are relatively basic functionality issues and threats, including the process in which these tokens are transferred across the network and how Ethereum users can be granted access to information regarding a particular token.

The benefits of using ERC-20 tokens include convenience and liquidity. Since the ERC20 regulations present a proper blueprint for developers to follow, it is easier for them to come up with tokens instead of starting from scratch.

There are far too many obstacles and gaps to fill in when creating tokens with specific functions from scratch. Aside from the token-creating process, there are also other tasks that developers need to spend considerable time in, which are creating safe wallets and applying for token listing on exchanges. There is also the threat of transferring tokens through broken contracts, which make the transaction process tedious and prone to hacks.

An important factor that is critical for the overall valuation of the Ethereum network is the liquidity of these ERC20 tokens. If the projects on top of Ethereum continuously become active and interconnected with each other, then it is going to bring more projects and more users to the Ethereum network, such the case with ADN.

As of May 2019, a total of 185,387 ERC-20 compatible tokens are found on the Ethereum main network. Within the Ethereum ecosystem, developers such as ADN, are allowed to interact between other tokens.

As mentioned above, ADN will be initially developed as an ERC-20 token, and developers will observe and test the token against possible technical flaws.

Once the ADN team has finished with the necessary preparations, and the developers have deemed the platform stable and secure, ADN will migrate from the Ethereum mainnet to its own blockchain.

ADN is currently developing its own blockchain, and the team is on the process of creating its own testnet. It will be adopting some of the cutting-edge features of prominent blockchain ecosystems such as Ethereum, EOS, and TRON. The team believes that there are commendable features & technologies from the aforementioned ecosystems, and we will improve on their technologies to create an ecosystem most conducive to the fulfillment of our purpose and structure.

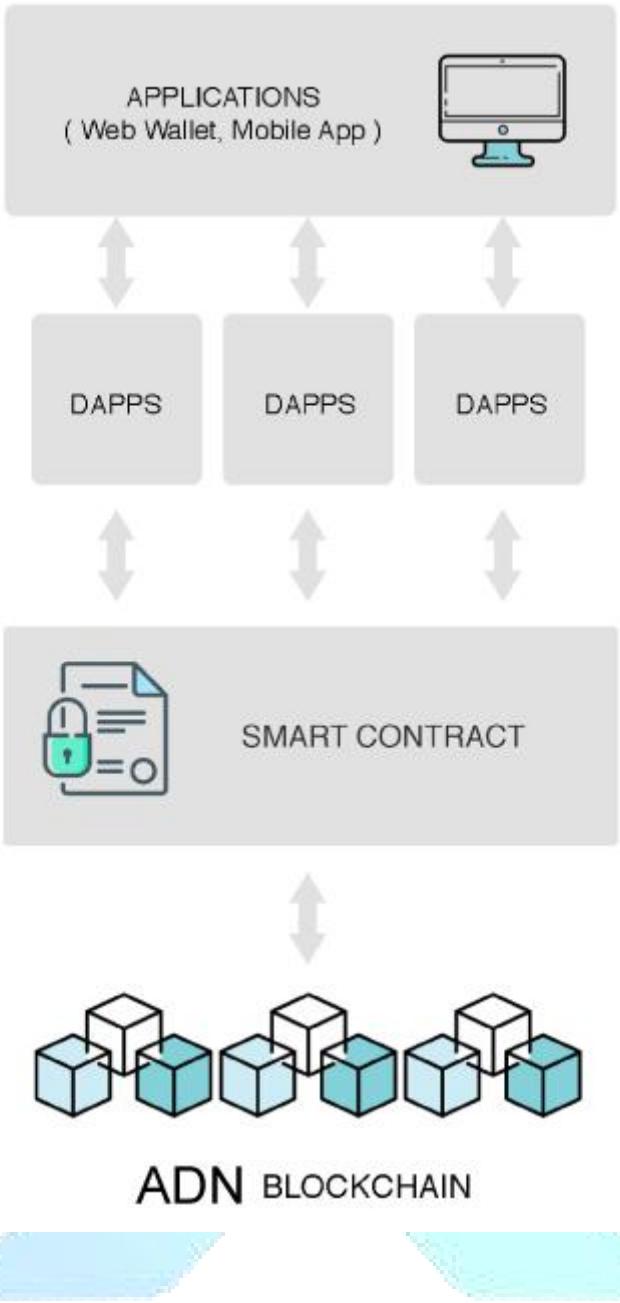
2.2 Core

ADN employs different modules in the core aspect, but it primarily focuses on smart contracts and consensus. ADN has its unique stack-based virtual machine, namely ADN Virtual Machine (AVM), and uses Solidity as its smart contract language. It implements Delegated Proof of Stake (DPoS), as it is proven to be the most efficient among presently-existing consensus mechanisms.

2.3 Application and Storage

The ADN protocol is created primarily to allow developers to create DApps on its blockchain. With the use of smart contracts, projects are funded by holding secured and investor-friendly ICOs.

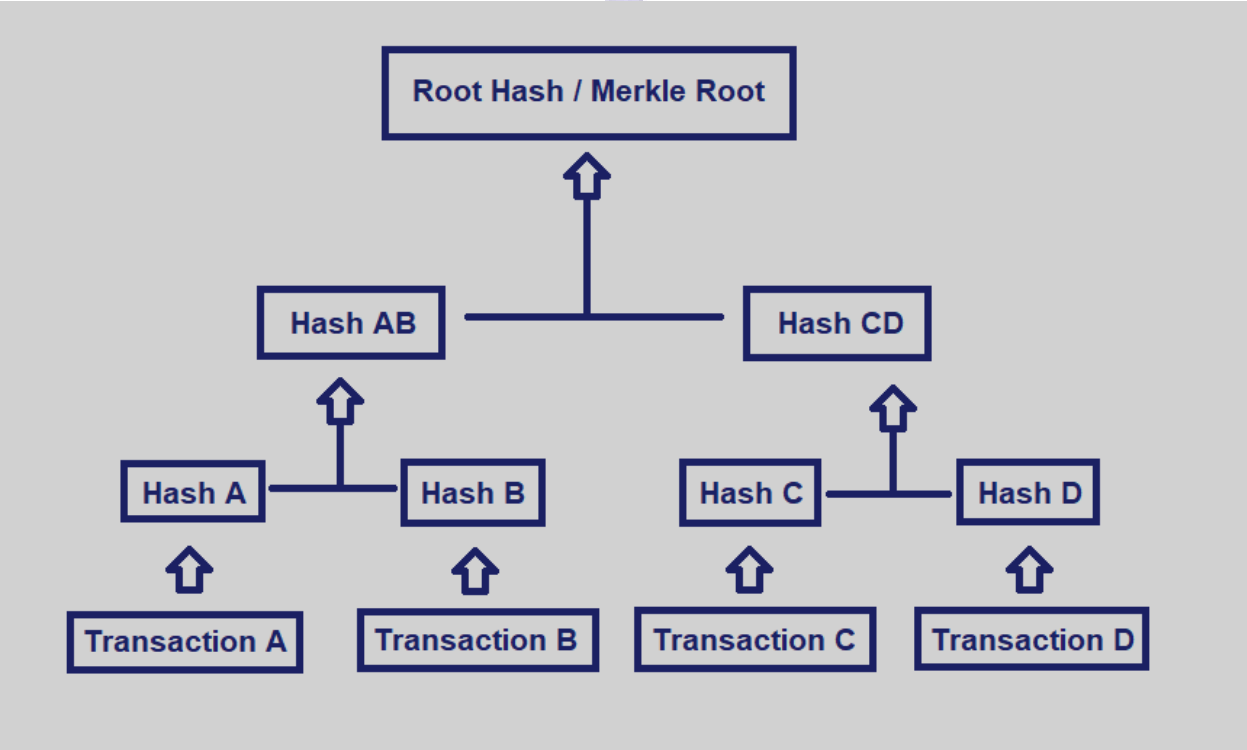
ADN blockchain will be using on-chain and off-chain DB to bank on the storage potential of offchain DB and decrease transaction weight. Once ICO is complete, and the DApp is running smoothly, developers can opt to migrate newly-minted chains to a separate main chain.


APPLICATIONS
(Web Wallet, Mobile App)
DAPPS
DAPPS
DAPPS
SMART CONTRACT
ADN BLOCKCHAIN

3. Consensus (DPoS)

3.1 Cryptographic Hashing

Bitcoin and Ethereum's consensus mechanism is called Proof of Work (PoW). Transactions in a PoW protocol is broadcasted through the network and grouped together into nascent blocks for confirmation from miners. The process of confirmation includes transaction hashing through cryptographic hashing algorithms until a merkle root has been reached, creating a merkle tree.



Below are properties of cryptographic hashing algorithms that are used to prevent any threat of network attacks:

- **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. But the reverse is not possible.

- **Collision resistance** - It is computationally improbable to locate any pairs x1 ≠ x2 such that h(x1) = h(x2). 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 x1, and thus h(x1), it is computationally improbable to locate any x2 such that h(x1) = h(x2). While this property is identical to collision resistance, this differs in that it is implying that an attacker with a given x1 will find it computationally improbable to locate any x2 hashing to the same output.
- **Deterministic** - maps each input to one and only one output.
- **Avalanche effect** - a small alteration in the input leads to a completely different output.

These are what provides the cryptocurrency network its intrinsic value by protecting the network from any possible sabotage.

Whenever miners confirm a newly-minted block, they are rewarded with tokens as a prize for participation in the network. But as the global crypto market capitalization increased, so did the miners who combined their resources to exponentially increase their computing potential. Miners also hoarded tokens as assets, rather than using them as Satoshi Nakamoto had originally envisioned in his Bitcoin whitepaper. Over time, GPU mining replaced the once-conventional CPU mining. This has been further replaced by ASICs, which are primarily created to mine specific cryptocurrencies. This drastic change created ramifications for miners regarding the amount of electricity needed to sustain mining operations as well as the hefty cost for the rig.

According to a study, the amount of electricity required for Bitcoin mining operation has been estimated to reach 3 GW[10]— equal to Ireland's power consumption. The study projects total power consumption to reach up to 8 GW in the future.

As a solution to the growing energy consumption crisis, the Proof of Stake (PoS) consensus mechanism was developed and promoted by many relatively newer networks. In this mechanism, holders of a certain token would "lock" or stake their token to become block validators. These validators take turns in proposing and validating future possible blocks, and if they do, new tokens are awarded to them as a reward. But the issue with this mechanism is that validator influence correlates directly to the number of tokens that have been staked by the validator. This has

resulted to groups of crypto miners that are hoarding massive amounts of the network's token to hold sway over the network's ecosystem and consensus.

3.2 Consensus Comparison

Features	DPoS	PoW	PoS
Incentivizing development	✓	✖	✖
Energy efficient	✓	✖	✖
Faster confirmation times	✓	✖	✖
Higher transaction volume	✓	✖	✓
Less incentives to centralize	✓	✖	✓

3.3 Proof of Work (PoW):

The Proof-of-Work consensus is the very first consensus algorithm. It uses a hash function to create conditions under which a single participant is permitted to announce their conclusions about the submitted information, and those conclusions can then be independently verified by all other system participants. The process of searching for valid 'hashes' (solutions to the 'hash function' created by the message input), is known as 'mining'.

Pros: Completely decentralized

Cons: Consume a lot of energy, low throughput

3.4 Proof of Stake (PoS)

The Proof-of-Stake consensus is similar to the PoW system. PoS replaces the hash function calculation with a digital signature which proves ownership of the first stake. The network selects an individual to approve new messages based on their proportional stake in the network.

Pros: High throughput

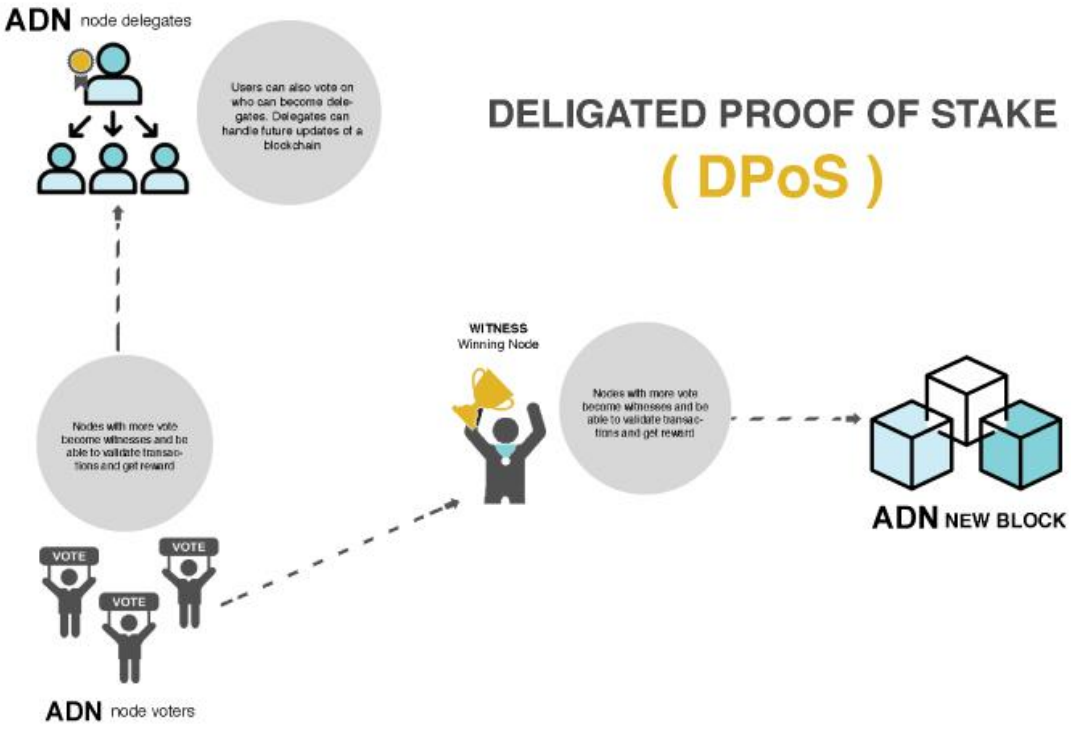
Cons: Nothing-at-Stake problem. By rewarding those who are already are most deeply involved in the network inherently creates an increasingly centralized system

3.5 Delegated Proof of Stake (dPoS)

ADN Platform will adapt the The Delegated Proof-of-Stake (dPoS) consensus. DPoS works similarly to the Proof-of-Stake system, with the addition of the ability of individuals to choose an overarching entity to represent their portion of stake in the system.

Pros: High throughput

Cons: Takes time to finalize and correct the chain if one of the master nodes fail in generating block.



4. Account

4.1 Account Types

The three types of accounts in the ADN Platform are regular accounts, token accounts, and contract accounts.

4.1.1 Regular accounts

Regular accounts are used for standard transactions. ICO companies will have regular accounts that can be utilized for normal transactions. These accounts can also trigger smart contracts for Decentralized Applications (DApps) development required for each participating body.

4.1.2 Token accounts

Token accounts are used for storing ARC-20 tokens. ICO companies can benefit from having a storage for their acquired ARC-20 tokens. These tokens are tokens of the ADN platform which

can be deployed for the investors' projects. Upon success of each ICO stage, ARC-20 token funds can then be accessed securely through the token accounts for further advancement.

4.1.3 Contract accounts

Contract accounts are smart contract accounts created by regular accounts. From ADN blockchain, business developers can create smart contract depending on their functions and projects in mind. Smart contracts created can merge on DApps per client requirements.

5. Block

5.1 Token and resource usage

There are 3 major categories where resources are consumed

1. Bandwidth and log storage
2. Computational backlog and computation power
3. State Storage

Blockchain maintains logs of each and every action and these actions are downloaded by all full nodes. Bandwidth and computation have two major components, instantaneous usage and long-term usage. Logs give us ability to walk back through to the genesis block.

6. Token

6.1 ARC-20 Token

ARC-20 is a technical standard used for smart contracts implementing tokens supported by the ADN Virtual Machine.

The interface is below:

```
contract ARC20Interface {
    function totalSupply() public constant returns (uint);
    function balanceOf(address tokenOwner) public constant returns (uint balance);
    function allowance(address tokenOwner, address spender) public constant returns (uint remaining);
    function transfer(address to, uint tokens) public returns (bool success);
    function approve(address spender, uint tokens) public returns (bool success);
    function transferFrom(address from, address to, uint tokens) public returns (bool success);
    event Transfer(address indexed from, address indexed to, uint tokens);
    event Approval(address indexed tokenOwner, address indexed spender, uint tokens);
}
```

7. Governance

Every member in the ADN ecosystem vie for the position of a Delegated Representative (DR), and there will be a total of 21 DR positions to fill. The members will be allowed to cast one vote per token, and those who earn the most votes will be assigned the position. The ecosystem will hold a vote every 6 hours, and should another member surpass any DR in terms of overall votes, the designation will change accordingly.

To add security measures against possible malicious attacks, the ecosystem has included a cost for members to become a DR candidate. When applying,10,000 ADN tokens will be burned from the candidate's account.

7.1 Block Reward

The 21 Delegated Representatives will share up to 230,000 ADN tokens as block rewards. Those who did not win enough votes to become part of the 21 DRs will share 115,000 ADN tokens up to the 100th candidate.

7.2 ADN Council

The ADN Council will be composed of the 21 DRs who will have the opportunity to improve ADN's network parameters, according to how they and the community see fit. For a new network parameter to be put into effect, the community will require at least 14 affirmative votes from the 21 DRs. The changes will reflect after 4 days. Prior to the implementation, members of the ADN ecosystem are required to perform the necessary actions they wish with the previous network parameters, as these changes will be irrevocable.

8. DApp Development

8.1 API

The ADN network will offer a wide selection of HTTP API gateways for interacting with the network via Full and Solidity Notes. Additionally, the team will develop a comprehensive JavaScript library containing API functions that enable developers to deploy smart contracts, change the blockchain state, query blockchain and contract information, trade, and much more. These API gateways can be directed towards a local privatenet or within the ADN platform.

8.2 Networks

Developers may connect to the networks by deploying nodes, interaction through using APIs or a developed service consisting of load balanced node clusters hosted on AWS servers worldwide. As DApp development scales up and API call volumes increase, the service successfully fields the increase in API traffic.

8.3 Tools

ADN offers an array of development tools for enabling developers to create innovative DApps. ADN will develop a framework that allows developers to test and deploy smart contracts via API. The service will be a load balance and hosted API service that allows developers to access the ADN network without having to run their own node. ADN will develop a comprehensive Integrated Development Environment that enables developers to compile, deploy and debug their Solidity smart contracts. It will contain an internal full node that creates a private local environment for smart contract testing prior to deployment. The API library connects developers to the network via a wide selection of HTTP API calls wrapped in JavaScript.

9. Conclusion

ADN will be a pioneering blockchain platform that will employ innovative methods for facing the challenges within blockchain networks. Not only will it be technically advanced, but it will also be considering the investors participating in the initial coin offerings in the ADN platform.