APOLLO

White Paper Version 1.0 – December 5, 2017

Contents

Abstract

Realizing the Potential of Blockchain

The internet is entering a second era that's based on blockchain. The last few decades brought us the internet of information. We are now witnessing the rise of the internet of value. Where the first era was sparked by a convergence of computing and communications technologies, this second era will be powered by a clever combination of cryptography, mathematics, software engineering and behavioural economics.

It is blockchain technology, also called distributed ledger technology. Like the internet before it, the blockchain promises to upend business models and disrupt industries. It is pushing us to challenge how we have structured society, defined value and rewarded participation.

What is Blockchain?

Each blockchain, like the one that uses bitcoin, is distributed: it runs on computers provided by volunteers around the world; there is no central database to hack or shut down. We can send money and soon any form of digitized value – from stocks and bonds to intellectual property, art, music and even votes – directly and safely between us without going through a bank, a credit-card company, PayPal or Western Union, social network, government or other middleman.

Blockchain is encrypted: it uses heavy-duty encryption involving public and private keys (rather like the two-key system to access a safety deposit box) to maintain virtual security.

In many cases, blockchain is public: anyone can view it at any time because it resides on the network, not within a single institution charged with auditing transactions and keeping records. No one can hide a transaction, and that makes bitcoin more traceable than cash.

Blockchain is, for the most part, inclusive. The blockchain through what he called "simplified payment verification" mode that can work on a mobile device. Now anyone with a flip phone can participate in the global economy; no documentation is required to be trusted.

Blockchain is immutable. Within minutes or even seconds, all the transactions conducted are verified, cleared and stored in a block that is linked to the preceding block, thereby creating a chain. Each block must refer to the preceding block to be valid. This structure permanently timestamps and stores exchanges of value, preventing anyone from altering the ledger.

Blockchain is historical. The blockchain is a distributed ledger representing a network consensus of every transaction that has ever occurred.

1. APOLLO Overview

For an entire electronic economy to be based on a fully decentralized, peer-to-peer solution, it must be able to do the following: process transactions securely, quickly and efficiently, at the rate of thousands per hour or more; provide incentives for people to participate in securing the network; scale globally with a minimal resource footprint; offer a range of basic transaction types that launch cryptocurrencies past the core feature of a payment system alone; provide an agile architecture that facilitates the addition of new core features, and allows for the creation and deployment of advanced applications; and be able to run on a broad range of devices, including mobile ones. APOLLO (pronounced “APO”) satisfies all these requirements.

APOLLO is a proof of stake (PoS) cryptocurrency, constructed from scratch in opensource Java. A total quantity of 10 billion available tokens were distributed in the genesis block. Curve25519 cryptography is used to provide a balance of security and required processing power, along with more commonly-used SHA256 hashing algorithms.

Blocks are generated every 60 seconds, on average, by accounts that are unlocked on network nodes. Since the full token supply already exists, APOLLO is redistributed through the inclusion of transaction fees which are awarded to an account when it successfully creates a block. This process is known as forging, and is akin to the “mining” concept employed by other cryptocurrencies. Transactions are deemed safe after 10 block confirmations, and APOLLO’s current architecture and block size cap allows for the processing of up to 367,200 transactions per day.

APOLLO transactions are based on a series of core transaction types that do not require any script processing or transaction input/output processing on the part of network nodes. These transaction primitives allow core support for:
• a fully-decentralized asset exchange
• alias creation, transfer and sale
• storage of small, optionally-encryptable strings of data on the blockchain
• a digital goods store
• account control features

By leveraging these primitive transaction types, APOLLO’s core can be seen as an agile, base-layer protocol upon which a limitless range of services, applications, and other currencies can be built.

Ongoing APOLLO development includes the implementation of a novel Transparent Forging feature which will allow a transaction processing capacity increase of two orders of magnitude using a deterministic block generation algorithm, coupled with additional network security mechanisms. The latest development roadmap also outlines the following short-term feature additions to the APOLLO core:

• a voting system
• asset exchange dividend payments
• a monetary system for facilitating the creation of new cryptocurrencies and associated services that are secured by the APOLLO blockchain

• atomic cross-chain trading, multi-signature transactions and escrow features
• additional mechanisms for securing the APOLLO blockchain, including penalties for accounts that do not behave as expected on the network

This version of the whitepaper documents features and algorithms that are implemented in APOLLO of version 1.0. Future revisions will be made to reflect additional planned features and algorithm changes.

2. Core technologies

2.1 Proof of Stake

In the traditional Proof of Work model used by most cryptocurrencies, network security is provided by peers doing “work”. They deploy their resources (computation/processing time) to reconcile double-spending transactions, and to impose an extraordinary cost on those who would attempt to reverse transactions. Tokens are awarded to peers in exchange for work, with the frequency and amount varying with each cryptocurrency’s operational parameters. This process is known as "mining". The frequency of block generation, which determines each cryptocurrency’s available mining reward, is generally intended to stay constant. As a result, the difficulty of the required work for earning a reward must increase as the work capacity of the network increases.

As a Proof of Work network becomes stronger, there is less incentive for an individual peer to support the network, because their potential reward is split among a greater number of peers. In search of profitability, miners keep adding resources in the form of specialized, proprietary hardware that requires significant capital investment and high ongoing energy demands. As time progresses, the network becomes more and more centralized as smaller peers (those who can do less work) drop out or combine their resources into "pools".

Bitcoin’s creator, Satoshi Nakamoto, intended for the bitcoin network to be fully decentralized, but nobody could have predicted that the incentives provided by Proof of Work systems would result in the centralization of the mining process. This leads to possible vulnerabilities. The GHash.io bitcoin pool has reached 51% of the bitcoin mining power in the past, and the top five bitcoin mining pools make up 70% of the Bitcoin network’s hashing power. The concept of decentralization is at risk of being completely lost.

In the Proof of Stake model used by APOLLO, network security is governed by peers having a stake in the network. The incentives provided by this algorithm do not promote centralization in the same way that Proof of Work algorithms do, and data shows that the APOLLO network has remained highly decentralized since its inception.

2.1.1 APOLLO's Proof of Stake Model

APOLLO uses a system where each "coin" in an account can be thought of as a tiny mining rig. The more tokens that are held in the account, the greater the chance that account will earn the right to generate a block. The total "reward" received as a result of block generation is the sum of the transaction fees located within the block. APOLLO does not generate any new tokens as a result of block creation. Redistribution of APOLLO takes place as a result of block generators receiving transaction fees, so the term "forging" (meaning in this context "to create a relationship or new conditions") is used instead of "mining".

Today, the block reward model also incorporates into APOLLO blockchain design (for details refer to 4.1 Reward Model).

Subsequent blocks are generated based on verifiable, unique, and almost-unpredictable information from the preceding block. Blocks are linked by virtue of these connections, creating a chain of blocks (and transactions) that can be traced all the way back to the genesis block.

Block generation time is targeted at 60 seconds, but variations in probabilities have resulted in an average block generation time of 80 seconds, with occasionally very long block intervals.

The security of the blockchain is always of concern in Proof of Stake systems. The following basic principles apply to APOLLO's Proof of Stake algorithm:

• A cumulative difficulty value is stored as a parameter in each block, and each subsequent block derives its new "difficulty" from the previous block's value. In case of ambiguity, the network achieves consensus by selecting the block or chain fragment with the highest cumulative difficulty. This is covered in more detail in 2.4.1.

• To prevent account holders from moving their stake from one account to another as a means of manipulating their probability of block generation, tokens must be stationary within an account for 1,440 blocks before they can contribute to the block generation process. Tokens that meet this criterion contribute to an account's effective balance, and this balance is used to determine forging probability.

• To keep an attacker from generating a new chain all the way from the genesis block, the network only allows chain re-organization 720 blocks behind the current block height. Any block submitted at a height lower than this threshold is rejected. This moving threshold may be viewed as APOLLO's only fixed checkpoint.

• Due to the extremely low probability of any account taking control of the blockchain by generating its own chain of blocks, transactions are deemed safe once they are encoded into a block that is 10 blocks behind the current block height.

2.2 Tokens

The total supply of APOLLO is 10 billion tokens, divisible to six decimal places.

The existence of anti-tokens in the genesis account has a couple of interesting side effects:

• the genesis account cannot issue transactions of any kind, since its balance is negative and it cannot pay transaction fees. As a result, the private passphrase for the genesis account is free for anyone to use.

• any tokens sent to the genesis account are effectively destroyed, since that account's negative balance will cancel them out. Several thousand APOLLO tokens have been burned in this manner.

• APOLLO assets may also be burned by transferring them to the genesis account. The choice of the word tokens is intentional due to APOLLO's intention to be used as a base protocol that provides numerous other functions. APOLLO's most basic function is one of a traditional payment system, but it was designed to do far more.

2.3 Network Nodes

A node on the APOLLO network is any device that is contributing transaction or block data to the network. Any device running the APOLLO software is seen as a node.

Nodes can be subdivided into two types: hallmarked and normal. A hallmarked node is simply a node that is tagged with an encrypted token derived from an account's private key; this token can be decoded to reveal a specific APOLLO account address and balance that are associated with a node. The act of placing a hallmark on a node adds a level of accountability and trust, so hallmarked nodes are more trusted than non-hallmarked nodes on the network. The larger the balance of an account tied to a hallmarked node, the more trust is given to that node. While an attacker might wish to hallmark a node in order to gain trustworthiness within the network and then use that trust for malicious purposes; the barrier to entry (cost of APOLLO required to build adequate trust) discourages such abuse.

Each node on the APOLLO network has the ability to process and broadcast both transactions and block information. Blocks are validated as they are received from other nodes, and in cases where block validation fails, nodes may be "blacklisted" temporarily to prevent the propagation of invalid block data.

Each node features built-in DDOS (Distributed Denial of Services) defence mechanisms which restrict the number of network requests from any peer to 30 per second.

2.4 Blocks

As in other cryptocurrencies, the ledger of APOLLO transactions is built and stored in a linked series of blocks, known as a blockchain. This ledger provides a permanent record of transactions that have taken place, and also establishes the order in which transactions have occurred. A copy of the blockchain is kept on every node in the APOLLO network, and every account that is unlocked on a node (by supplying that account's private key) has the ability to generate blocks, as long as at least one incoming transaction to the account has been confirmed 1,440 times. Any account that meets these criteria is referred to as an active account.

In APOLLO, each block contains up to 255 transactions, all prefaced by a 192-byte header that contains identifying parameters. Each transaction in a block is represented by a maximum of 128 bytes, and the maximum block size is 256KB.

All blocks contain the following parameters:

- A block version
- A block timestamp, expressed in seconds since the genesis block
- The ID and hash of the previous block
- The number of transactions stored in the block
- The total amount of APO transaction volumes in the block
- The total amount of transaction fees in the block
- The payload length of the block
- The hash value of the block payload
- The account's public key generated by the block
- The block's generation signature
- A signature for the entire block

2.4.1 Block Creation (Forging)

Three values are key to determining which account is eligible to generate a block, which account earns the right to generate a block, and which block is taken to be the authoritative one in times of conflict: base target value, target value and cumulative difficulty.

Base Target Value In order to win the right to forge (generate) a block, all active APOLLO accounts "compete" by attempting to generate a hash value that is lower than a given base target value. This base target value varies from block to block, and is derived from the previous block's base target value multiplied by the amount of time that was required to generate that block.

Target Value Each account calculates its own target value, based on its current effective stake. This value is:

$$T = Tb \times S \times Be$$

where:
T is the new target value

Tb is the base target value
S is the time since the last block, in seconds
Be is the effective balance of the account

As can be seen from the formula, the target value grows with each second that passes since the timestamp of the previous block. The maximum target value is $1.53722867 \text{ x } 10^{17}$ and the minimum target value is one half of the previous block's base target value.

This target value and the base target value are the same for all accounts attempting to forge on top of a specific block. The only account-specific parameter is the effective balance parameter.

Cumulative Difficulty The cumulative difficulty value is derived from the base target value, using the formula:

$$\text{Dcb} = \text{Dpb} + \frac{2^{64}}{\text{Tb}}$$

where:
Dcb is the difficulty of the current block
Dpb is the difficulty of the previous block
Tb is the base target value for the current block

The Forging Algorithm
Each block on the chain has a generation signature parameter. To participate in the block forging process, an active account cryptographically signs the generation signature of the previous block with its own public key. This creates a 64-byte signature, which is then hashed using SHA256. The first 8 bytes of the resulting hash gives a number, referred to as the account's "Hit.

The Hit is compared to the current target value. If the computed Hit is lower than the target, then the next block can be generated. As noted in the target value formula, the target value increases with each passing second. Even if there are only a few active accounts on the network, one of them will eventually generate a block because the target value will become very large. The corollary of this is that user can estimate the time that will be required for any account to forge a block by comparing that account's Hit value to the target value.

The last point is significant. Since any node can query the effective balance for any active account, it is possible to iterate through all active accounts in order to determine their individual Hit value. This means it is possible to predict, with reasonable accuracy, which account will next win the right to forge a block.

A shuffling attack could be mounted by moving stake to an account that will generate the next block, which is another reason why a APOLLO stake must be stationary for 1,440 blocks before it can contribute to forging (via the effective balance value). Interestingly, the new base target value for the next block cannot be reasonably predicted, so the nearly-deterministic process of determining who will forge the next block becomes increasingly stochastic as attempts are made to predict future blocks.

This feature of the APOLLO forging algorithm helps form the basis for the development and implementation of the Transparent Forging algorithm.

When an active account wins the right to generate a block, it bundles up to 255 available, unconfirmed transactions into a new block, and populates the block with all of its required parameters. This block is then broadcast to the network as a candidate for the blockchain.

The payload value, generating account, and all of the signatures on each block can be verified by all network nodes who receive it. In a situation where multiple blocks are generated, nodes will select the block with the highest cumulative difficulty value as the authoritative block. As block data is shared between peers, forks (non-authoritative chain fragments) are detected and dismantled by examining the chains' cumulative difficulty values stored in each fork.

There are two conditions that an account needs to satisfy before it can start forging:

The account needs to have an effective balance of at least 1,000,000 APO. That is, it needs to have had a balance of 1,000,000 APO (or more) over the last 1440 blocks / 24 hours. This is needed because the forging algorithm depends on the stake of the user. The account needs to have at least one outgoing transaction, also confirmed 1440 times.

The passphrase is the the account's private key, a public key is obtained only after at least one outgoing transaction is executed and confirmed. This can be done in several ways, notably by sending 1 APO to your own account (or someone else's), by sending message using the crypto messaging feature or by registering an alias.

When these two conditions are met, a 1,000,000 APO effective balance and public key published, the account is eligible to forge.

Note that forging will stop if the effective balance drops below 1,000,000 APO.

Balance leasing
Since the ability for an account to forge is based on the effective balance parameter, it is possible to "loan" forging power from one account to another without giving up control of the tokens associated with the account. Using a transaction of the "account control" type, an account owner may temporarily reduce an account's effective balance to zero, adding it to the effective balance of another account. The targeted account's forging power is increased until the end of a time period specified by the original account owner, after which the effective balance is returned to the original account.

Accounts with leased forging power generate blocks more often and earn more transaction fees, but those fees are not automatically returned to lease accounts. With a bit of coding, however, this system allows for the creation of nearlytrustless forging pools that can make payouts to participants.

2.4.2 Accounts

APOLLO implements a brain wallet as part of its design: all accounts are stored on the network, with private keys for each possible account address directly derived from each account's passphrase using a combination of SHA256 and Curve25519 operations.

Each account is represented by a 64-bit number, and this number is expressed as an account address using a Reed-Solomon error-correcting notation that allows for detection of up to four errors in an account address, or correction of up to two errors. This format was implemented in response to concerns that a mistyped account address could result in tokens, aliases, or assets being irreversibly transferred to erroneous destination accounts. Account addresses are always prefaced by "APO-", making APOLLO account addresses easily recognizable and distinguishable from address formats used by other cryptocurrencies.

The Reed-Solomon-encoded account address associated with a secret passphrase is generated as follows:

1. The secret passphrase is hashed with SHA256 to derive the account's private key.
2. The private key is encrypted with Curve25519 to derive the account's public key.
3. The public key is hashed with SHA256 to derive the account ID.
4. The first 64 bits of the account ID are the visible account number.
5. Reed-Solomon encoding of the visible account number, prefixed with "APO-", generates the account address.

When an account is accessed by a secret passphrase for the very first time, it is not secured by a public key. When the first outgoing transaction from an account is made, the 256-bit public key derived from the passphrase is stored on the blockchain, and this secures the account. The address space for public keys (2^256) is larger than the address space for account numbers (2^64), so there is no one-to-one mapping of passphrases to account numbers and collisions are possible. These

collisions are detected and prevented in the following way: once a specific passphrase is used to access an account, and that account is secured by a 256-bit public key, no other public-private key pair is permitted to access that account number.

Account Balance Properties. For each APOLLO account, several different types of balances are available. Each type serves a different purpose, and many of these values are checked as part of transaction validation and processing.

• The effective balance of an account is used as the basis for an account's forging calculations. An account's effective balance consists of all tokens that have been stationary in that account for 1,440 blocks. In addition, the Account Leasing feature allows an account's effective balance to be assigned to another account for a temporary period.
• The guaranteed balance of an account consists of all tokens that have been stationary in an account for 1,440 blocks. Unlike the effective balance, this balance cannot be assigned to any other account.

• The basic balance of an account accounts for all transactions that have had at least one confirmation.

• The forged balance of an account shows the total quantity of APOLLO that have been earned as a result of successfully forging blocks.

• The unconfirmed balance of an account is the one that is displayed in APOLLO clients. It represents the current balance of an account, minus the tokens involved in unconfirmed, sent transactions.

• Guaranteed asset balances lists the guaranteed balances of all the assets associated with a specific account.

• Unconfirmed asset balances lists the unconfirmed balances of all the assets associated with a specific account.

2.4.3 Transactions

Transactions are the only means APOLLO accounts have of altering their state or balance. Each transaction performs only one function, the record of which is permanently stored on the network once that transaction has been included in a block.

Transaction Fees. Transaction fees are the primary mechanism through which APOLLO are recirculated back into the network. Every transaction requires a minimum fee of 0.01 APOLLO; currently, the only exception is the fee for issuing an asset on the APOLLO Asset Exchange, which is 5,000 APOLLO. When a APOLLO account forges a block, all of the transaction fees included in that block are awarded to the forging account as a reward.

Until the size of all the transactions in a block exceeds the current 256 kilobyte block size limit, the minimum fee will be sufficient for all transactions to be included in blocks. In situations where the number of unconfirmed transactions exceeds the number that can be placed in a block, forging accounts will likely select transactions with the highest fees. This suggests that transaction processing may be prioritized by including a fee that is higher than the minimum.

Transaction Confirmations. All APOLLO transactions are considered unconfirmed until they are included in a valid network block. Newly-created blocks are distributed to the network by the node (and associated account) that creates them, and a transaction that is included in a block is considered as having received one confirmation. As subsequent blocks are added to the existing blockchain, each additional block adds one more confirmation to the number of confirmations for a transaction.

If a transaction is not included in a block before its deadline, it expires and is removed from the transaction pool.

Transaction Deadlines. Every transaction contains a deadline parameter, set to a number of minutes from the time the transaction is submitted to the network. The default deadline is 1,440 minutes (24 hours). A transaction that has been broadcast to the network but has not been included in a block is referred to as an unconfirmed transaction.

If a transaction has not been included in a block before the transaction deadline expires, the transaction is removed from the network.

Transactions may be left unconfirmed because they are invalid or malformed, or because blocks are being filled will transactions that have offered to pay higher transaction fees. In the future, features such as multi-signature transactions may be able to take advantage of deadlines as a means of enforcing an expiry date.

Transaction Types Categorizing APOLLO transactions into types and subtypes allows for modular growth and development of the APOLLO protocol without creating dependencies on other “base” functions. As features are added to the APOLLO core, new transaction types and subtypes can be added to support them.

The following five transaction types and associated subtypes are supported by APOLLO. Each type dictates a given transaction’s required and optional parameters, as well as its processing method.

1. Payment: used for sending APOLLO tokens from one account to another
• Ordinary payment

2. Messaging: used by messaging, alias, voting, and account info features
• Arbitrary message
• Alias assignment
• Poll creation
• Vote casting
• Account info

3. Colored coins: an implementation of the colored coins concept, which enables the APOLLO Asset Exchange

- Asset issuance
- Asset transfer
- Ask order placement
- Bid order placement
- Ask order cancellation
- Bid order cancellation

4. Digital Goods: transactions that enable the APOLLO Digital Goods store

- Listing
- Delisting
- Price change
- Quantity change
- Purchase
- Delivery
- Feedback
- Refund

5. Account control: transactions that place limits on how accounts may or may not be used.

• Effective balance leasing

Transaction Creation and Processing. The details of creating and processing a APOLLO transaction are as follows:

1. The sender specifies parameters for the transaction. Types of transactions vary18, and the desired type is specified at transaction creation, but several parameters must be specified for all transactions:

- the private key for the sending account
- a specified fee for the transaction
- a deadline for the transaction
- an optional referenced transaction

2. All values for the transaction inputs are checked. For example, mandatory parameters must be specified; fees cannot be less than or equal to zero; a transaction deadline cannot be less than one minute into the future; if a referenced transaction is specified, then the current transaction cannot be processed until the referenced transaction has been processed.

3. If no exceptions are thrown as a result of parameter checking:

(a) The public key for the generating account is computed using the supplied secret passphrase

(b) Account information for the generating account is retrieved, and transaction parameters are further validated:

• The sending account's balance cannot be zero

• The sending account's unconfirmed balance must not be lower than the transaction amount plus the transaction fee

4. If the sending account has sufficient funds for the transaction:
(a) A new transaction is created, with a type and subtype value set to match the kind of transaction being made. All specified parameters are included. A unique transaction ID is generated with the creation of the object
(b) The transaction is signed using the sending account's private key
(c) The encrypted transaction data is placed within a message instructing network peers to process the transaction
(d) The transaction is broadcast to all peers on the network
(e) The server responds with a result code:
- the transaction ID, if the transaction creation was successful
- an error code and error message if any of the parameter checks fail.

2.5 Cryptographic Foundations

Key exchange in APOLLO is based on the Curve25519 algorithm, which generates a shared secret key using a fast, efficient, high-security elliptic-curve Diffie-Hellman function. The algorithm was first demonstrated by Daniel J. Bernstein in 2006.

Message signing in APOLLO is implemented using the Elliptic-Curve Korean Certificate based Digital Signature Algorithm (EC-KCDSA), specified as part of IEEE P1363a by the KCDSA Task Force team in 1998.

Encryption Algorithm

When Alice sends an encrypted plaintext to Bob, she:

1. Calculates a shared secret:
    - shared_secret = Curve25519(Alice_private_key, Bob_public_key)

2. Calculates N seeds:
    - seedn = SHA256(seedn-1), where seed0 = SHA256(shared_secret)

3. Calculates N keys:
    - keyn = SHA256(Inv(seedn)), where Inv(X) is the inversion of all bits of X

4. Encrypts the plaintext:
    - ciphertext[n] = plaintext[n] XOR keyn

Upon receipt Bob decrypts the ciphertext:

1. Calculates a shared secret:
    - shared_secret = Curve25519(Bob_private_key, Alice_public_key)

2. Calculates N seeds (this is identical to Alice's step):
    - seedn = SHA256(seedn-1), where seed0 = SHA256(shared_secret)

3. Calculates N keys (this is identical to Alice's step):
    - keyn = SHA256(Inv(seedn)), where Inv(X) is the inversion of all bits of X

4. Decrypts the ciphertext:
    - plaintext[n] = ciphertext[n] XOR keyn

Note: If someone guesses part of the plaintext, he can decode some part of subsequent messages between Alice and Bob if they use the same key pairs. As a result, it's advised to generate a new pair of private/public keys for each communication.

3. Core Features

3.1 Basic Payments

The most fundamental feature of any cryptocurrency is the ability to transmit tokens from one account to another. This is APOLLO's most fundamental transaction type, and it allows for basic payment functionality.

3.2 Crypto Messaging

Crypto Messaging strings of data up to 1,000 bytes in length can be stored on the APOLLO blockchain using the Crypto Messaging feature. These messages are intended to be removable, in the future, when blockchain size needs to be reduced; nonetheless, they form a critical building block for a number of next-generation features. At the basic level, the system can be used to transmit human-readable messages between accounts, creating a decentralized chat system.

3.3 Asset Exchange

An entire class of APOLLO transactions is used to implement a fully-decentralized and automated asset exchange that operates on the APOLLO blockchain. Using the colored coins concept, APOLLO assets may be issued and tracked on the APOLLO ecosystem, supported by transactions and processing that allow for asset transfer, bid and ask order placement, and automatic order matching.

By combining the features of the APOLLO Asset Exchange with other features such as Crypto Messaging, value-added services can be created.

3.4 P2P Marketplace

The APOLLO P2P Marketplace gives account owners the ability to list assets for sale in an open, decentralized market place. Goods can be purchased, discounted, delivered, refunded, and transferred, using a dedicated class of transaction types that manage and secure store listings on the decentralized blockchain.

3.5 Device Portability

Due to its cross-platform, Java-based roots, its Proof of Stake hashing and its future ability to reduce the size of the block chain, APOLLO is extremely well suited for use on small, low-power, low-resource devices. Android and iPhone applications are currently in development.

The ability to implement APOLLO on low-powered, always-connected devices such as smartphones allows us to envision a scenario where the majority of the APOLLO network is supported on mobile devices. The low cost and resource consumption of

these devices significantly reduce network costs in comparison with traditional Proof of Work cryptocurrencies.

4. Proof of Work vs Proof of Stake

In comparison, in a Proof of Work (PoW) model, a reward is given for undertaking complex computational work involving solving problems. This exercise is termed as “mining” and people who undertake this work are called “miners”. Miners compete with each other to find solutions to problems and are rewarded whenever they are able to do so first. In theory, this is a wonderful principle but it requires complex hardware and a lot of electricity to run this hardware.

Unlike the PoW however, with the Proof of Stake (PoS) model, the creator of each block is determined by the wealth it holds, PoS is a different way to validate transactions based and achieve the distributed consensus. PoS system is faster and more economical than PoW, as it reduces energy costs and makes it possible to forge using even an ordinary laptop.

4.1 Reward Model

Generally, there are no block rewards involved for PoS, so the forgers can only get the transaction fees. Today, APOLLO has effectively combined the two factors into considerations. A forger of APOLLO can now enjoy the chances to forge blocks that contain transaction fees and also block rewards!

APOLLO blockchain, the first ever cryptocurrency based on a provably secure and scalable blockchain design by incorporating the PoW concept into PoS mechanisms. It is far more robust than that in a pure PoS based system where only transaction fees be rewarded.

The APOLLO block reward incentive makes APOLLO a robust blockchain that attract more nodes to become forgers as greater chances to be rewarded by securing the network. Having more nodes in a blockchain indicates that more secure of APOLLO network can be.

It makes APOLLO the best of both worlds!

A premine is where a developer allocates a certain amount of currency credit to a particular address before releasing the source code to the open community. With only 40% of premined coins, it means that at the time the APOLLO coin start to be used, the majority of 60% of APOLLO are the block rewards have yet to be “forged” by anyone. In a blockchain where no one could have already got an unreasonably large amount of APOLLO, therefore how APOLLO be distributed to people becomes a fairer deal. The design of APOLLO blockchain provides a greater room of opportunities!

Forging is needed to make things secure but without an incentive to perform forging, no one will do it. Therefore, when an APOLLO account forges a block, all of the transaction fees included in that block will be awarded to the forging account together with the block reward. By accumulating more APOLLO, it also increases the chances to forge a block based on PoS mechanism.

4.1.1 What is the APOLLO Forging Block Reward?

The APOLLO block reward refers to the APOLLO distributed by the network to forgers for each successfully solved block.

4.1.2 How is the Block Reward Determined?

APOLLO Team, APO's creator, set the block reward schedule when they created APOLLO. It is one of APOLLO's central rules and cannot be changed without agreement between the entire APOLLO network.

The block reward started at 1,000 APO in block #1 and reduced by 10% for every 1,000,000 blocks. This means every block up until block #1,000,000 rewards 1,000 APO, while block 1,000,001 rewards 900, block 2,000,001 rewards 810, block 3,000,001 rewards 729 APO and so on. Since blocks are forged on average every 60 seconds, 1,440 blocks are forged per day on average. At 1,440 blocks per day, 1,000,000 blocks take on average 1.9 years to forge and approximately 16 years to finish the overall "forging" process.

4.1.3 Importance of the Block Reward

The block reward creates an incentive for forgers to add hash power to the network.

It is worth mentioning that, the block reward can now be forged by forgers using their computer without incurred high electricity costs, which make up the entirety of the APOLLO network hash rate. Also, forgers who successfully forge APOLLO can also sell them for a profit in APOLLO decentralized exchange.

Conclusion

The Transformation of Blockchain Technology

Now many people will ask such a question, bitcoin can only deal with 7 transactions per second, so how can the low transaction efficiency bring about technical changes? In fact, there is a big misunderstanding here. Remember during the early days of internet, the speed of dial-up internet is only few kb per second, download a MP3 requires more than 10 minutes. However, you cannot say this is useless.

Many disruptive technologies go through an immature to maturity stage. Like many early disruptive technologies, the most typical one is the internet bubble around Year 2000 and after the bubble, people find out that the internet in the early days is not so magical, nor to penetrate into various sectors. When a technological invention has not reached the point where large-scale commercial applications can erupt, especially where infrastructure and popularity are still immature, many different points of view arise. But the seed of the really great internet company was also planted during that time. History has proved how powerful the advance of science and technology is.

Today, APOLLO is an open source project with a core development team who are doing various R & D and upgrade programs. An investment with 10 times or even 100 times return on investment opportunities is achievable so long as the investor is able to spot on the valuable digital assets with good growth potential. APOLLO, with its smart contract features and blockchain technology as an evolutionary version, is a wakeup digital asset market.

Bitcoin is already a success proven model, except that its technology is still unable to do smart contracts and smart transactions. At the time of writing this white paper, the market value of Bitcoin has been as high as $186 billion. APOLLO, which is known for its blockchain-based innovation platform, has a 10 billion limit. With the birth of many innovative blockchain agreements, Bitcoin is no longer the single-only digital asset. Innovation agreements and blockchain applications will be the next investment theme.

So APOLLO is to repeat its success in a shorter time to achieve greater breakthroughs, or even better than the previous Bitcoin's amazing results.

References

[1] Bitcoin: a Peer-to-Peer Electronic Cash System. (n.d.). Retrieved December 5, 2017, from https://bitcoin.org/bitcoin.pdf
[2] Bitcoin Is Broken. (n.d.). Retrieved December 5, 2017, from http://hackingdistributed.com/2013/11/04/bitcoin-is-broken/
[3] Bitcoin Miners Ditch Ghash.io Pool Over Fears of 51% Attack. (n.d.). Retrieved December 5, 2017, from http://www.coindesk.com/bitcoin-minersditch-ghash-io-pool-51-attack/
[4] Bitcoin needs to scale by a factor of 1000 to compete with Visa. Here's how to do it. (n.d.). Retrieved December 5, 2017, from http://www.washingtonpost.com/blogs/theswitch/wp/2013/11/12/bitcoin-needs-to-scale-by-a-factor-of-1000-tocompete-with-visa-heres-how-to-do-it/
[5] Bitcoin security guarantee shattered by anonymous miner with 51% network power. (n.d.). Retrieved December 5, 2017, from https://arstechnica.com/information-technology/2014/06/bitcoin-security-guarantee-shattered-by-anonymous-miner-with-51-network-power/
[6] Cohen, R. (2013, December 28). Global Bitcoin Computing Power Now 256 Times Faster Than Top 500 Supercomputers, Combined! Retrieved December 5, 2017, from http://www.forbes.com/sites/reuvencohen/2013/11/28/globalbitcoin-computing-power-now-256-times-faster-than-top-500-supercomputers-combined
[7] Crypto Review of Curve25519.java & Crypto.java. (n.d.). Retrieved December 5, 2017, from https://gist.github.com/doctorevil/9521116
[8] Eyal, I., & Gun Sirer, E. (2013). Majority is not Enough: Bitcoin Mining is Vulnerable. Unpublished manuscript. Retrieved December 5, 2017, from http://arxiv.org/pdf/1311.0243v5.pdf
[9] Learn Cryptography — 51% Attack. (n.d.). Retrieved December 5, 2017, from http://learncryptography.com/51-attack/
[10] Losing to win. (2017, June 23). Retrieved December 5, 2017, from http://www.economist.com/blogs/schumpeter/2017/06/bitcoin
[11] Peercoin. (n.d.). Retrieved December 5, 2017, from http://www.peercoin.net/whitepaper
[12] Qin, W., & Zhou, N. (2010, 12). New concurrent digital signature scheme based on the computational Diffie-Hellman problem. The Journal of China Universities of Posts and Telecommunications, 17(6), 89-100. doi: 10.1016/S1005-8885(09)60530-6
[13] The Well Deserved Fortune of Satoshi Nakamoto, Bitcoin creator, Visionary and Genius. (n.d.). Retrieved December 5, 2017, from http://bitslog.wordpress.com/2013/04/17/the-well-deserved-fortune-ofsatoshi-nakamoto/
[14] Yung, M., Dodis, Y., Kiayias, A., Malkin, T., & Bernstein, D. J. (2006). Curve25519: New Diffie-Hellman Speed Records. Public Key Cryptography, 2006, 207-228. doi: 10.1007/11745853_14