Digital Asset Solution Coin (DAS)

Whitepaper v1.0

Created by Digital Asset Solution Coin Community

April 29, 2020

Abstract

Digital currency, represented by Bitcoin and Ethereum, is blazing through traditional financial systems with the force of a prairie fire. Bitcoin has proven that a peer-to-peer electronic cash system can work and fulfill payments processing without requiring trust or a central mint. However, to be able to fully accommodate the traditional financial business needs to be based on a fully decentralized, peer-to-peer solution, it will strongly need to expand the capability to manage following activity: securely, quickly and efficiently processing transactions, fast enough to manage huge amount of transaction at the rate of thousands per hour or more; provide best incentives model for people to participate in securing the network; scalability at global stage 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 any additional core features, and allows for the creation and be able to run on a wide range of devices, including mobile. Digital Asset Solution Coin satisfies all these requirements.

1. Introduction and Overview

Digital Asset Solution Coin is a proof-of-stake cryptocurrency. Digital Asset Solution Coins has its unique proof-of-stake algorithm different way of design comparing with any implementation of the coin age concept used by other proof-of-stake cryptocurrencies and is resistant to so-called nothing at stake attacks. A total quantity of 1 billion available coins were distributed in the genesis block. Curve25519 cryptography is used to provide a balance of security and required processing power, along with the used of SHA256 hashing algorithms.

Generating Blocks in every 60 seconds, on average, by independent accounts on network nodes. Since the full token supply already exists, Digital Asset Solution Coin is redistributed with 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 like the mining concept that are used by other cryptocurrencies. Transactions are deemed safe after 30 block confirmations, and with the Digital Asset Solution Coins current architecture and block size cap allows for the processing of up to 300.000 transactions per day.

Digital Asset Solution Coin transactions are based on a series of core transaction types that are not require any of script processing or transaction input/output processing at the network nodes side. These transactions allow core support for: asset exchange, alias registration, encrypted messages, digital goods store, monetary system, voting system, phased transactions, account control, shuffling, account properties, cloud data

Digital Asset Solution Coins core can be recognized as an agile, base-layer protocol upon which a limitless range of services, applications, and other currencies can be built.

1.1 Technology Background

Existing blockchain contracts can only perform simple smart contract computations, the blockchain addresses the transmission and accounting of decentralized value networks. Bitcoin uses a SHA256 Proof of Work (PoW) for consensus on the computational contribution, with each block divided into three parts, namely:

1. The hash value of the last block serves as the block header of the current block.
2. Pending transactions (*t*1, *t*2,_ _ _,*tn*) within the time window *T* will be hashed into block Coinbase; and
3. Including miner's address, which is normally the address of mining pool, the *X*, as the input of hash functions, will be dispatched by pool server to each miner, who will complete certain computations. The goal is to find *H* (*X;* nonce) < Target

Difficulty, where nonce is an appended randomized guessing number. The computation result will be verified by the whole network nodes so as to get the reward out of the block to the exact miner's address, and then the whole network enters the computation of the next block, thus forming a chain eventually. In addition, there are some other information, such as version number, Merkle tree, timestamp, etc.

The whole mining process can be summarized as:

SHA256(SHA256(version+prev_hash+merkle_root+ntime+nbits+nonce)) < TARGET
Ethereum makes use of uncle blocks [4] to improve network concurrency. In particular, both the Ethereum network and the Rootstock [5] network is designed for smart contracts on the chain. The consensus and tamper-proof of make blockchain automatically ensures the enforcement of the contract, contract execution, and funds allocation, thus eliminating the trust and dependence on people or other third parties.

In the process of optimizing the objective function, various numerical methods are often used to iteratively gradient descent to find the global optimal solution. Large-scale distributed learning often adopts ASGD (asynchronous stochastic gradient descent) to optimize the results. Sometimes, for particular problems, the training can only obtain a sub-optimal solution at a certain distance from the global optimum according to a distribution.

Instead of PoW (proof-of-work), Digital Asset Solution Coin relies (PoS) Proof-of-Stake algorithm to reach consensus. But what is the difference?

Cryptocurrencies such as Bitcoin which use PoW, require mining. To mine, expensive computer hardware is required and utilized to solve very complex mathematical problems to earn the rewards. It's considered very expensive.

On the other hand, under PoS creators of new blocks are selected deterministically-based on their wealth. This is far much more cost-effective. The other implication here is that since Digital Asset Solution Coin does not require mining, there is a static supply of money.

In addition, the network is less susceptible to hacks. To hack a PoS network, hackers would need to invest massive amounts of the currency, and this is likely to devalue their holdings.

The Digital Asset Solution Coin ecosystem is fueled by Digital Asset Solution Coin as its virtual currency. Digital Asset Solution Coin tokens can be used for the following:

- To cover transaction fees when transferring Digital Asset Solution Coin between users.
- Creating assets representing bonds or ownership of projects.
- Deploy decentralized polls within a Blockchain.
- As a digital currency for exchange during ordinary purchases

2. Purpose

The value of Bitcoins is constantly fluctuating according to demand. This constant fluctuation will cause Bitcoin accepting sites to continually change prices. It will also cause a lot of confusion if a refund for a product is being made. For example, if a t-shirt was initially bought for 1.5 BTC, and returned a week later, should 1.5 BTC be returned, even though the valuation has gone up, or should the new amount (calculated according to current valuation) be sent? Which currency should BTC tied to when comparing valuation? These are still important questions that the Bitcoin community still has no consensus over.

Digital Asset Solution Coin purpose is to develop more stable coin environment. In which every coin of Digital Asset Solution Coin will be backed up by real asset that are offered in the marketplace. One which is trade at the marketplace is the tokens not the coin itself. Every transaction related to token trading will be subject for a fee in the form of Digital Asset Solution Coin coins.

3. Coin Distribution

3.1 Coin Allocations

1 (One) Billion coins are generated at the same time of Genesis block creation.

11 (Eleven) Genesis Accounts also created in purpose to make sure the system is well and stable running operation in the early stage of the DAS release. The 11 Genesis Account is separated to 2 function such as:

- 1 Genesis Account as *Reserve Account*
- 10 Genesis Accounts as *Forger Account*.

From the total of 1 Billion coins, *900 Million coins* are stored in *Reserve Account* and total of *100 Million coins* are reserved for *Forger Accounts*. In other words, Forger Account reserved 10 Million coins for each.

Coin Distribution Ratio

Available (distributed for sell)	**90%**
Reserve for forging account (not distributed for sell)	**10%**

No additional new coin will be added in the future, total coin quantity will always be as much as 1 Billion coins.

3.2 Genesis Accounts

In order to maintain transparency, Digital Asset Solution Coin reveal information regarding the genesis account and its use as follows.

- ***Reserve Account***

1. DAS-NXH5-QTFG-MPKJ-58C92

- ***Forger Account***

1. DAS-8CMC-MYW6-Y4SA-HDYUL
2. DAS-CB6R-5NUQ-HDK7-C9YN5
3. DAS-64KN-6AMA-3AC8-8N5GF
4. DAS-SEPV-UFSR-WY5P-5NA4X
5. DAS-9AD3-UASE-6XDH-DJPRS
6. DAS-VXE8-ZL8G-RDBJ-38A67
7. DAS-7C32-QQ56-DKFD-GSV6X
8. DAS-L9F4-QZM2-57FM-9SNCC
9. DAS-7QC4-FGUB-YJTG-7M2UF
10. DAS-VM87-F6BK-DTY3-5779K

4. Core technologies

4.1 Proof of Stake

Proof-of-Stake (PoS) is a system on the same basis as Proof-of-Work (PoW), but has several advantages, including the acceleration of a validation process. This type of algorithm is used to reach a distributed consensus, which is chosen through various combinations of random choices based on the amount of Hash power the miner has. The application of PoS algorithm in cryptography uses computationally intensive puzzles for transaction validation and the creation of new blocks. Proof-of-Stake has been favored as a more flexible consensus system with modifications from developers. Nxt and BlackCoin use make modifications in the formula to find the lowest hash value combined. That is, the division of the mining process (validation) can be done evenly, not like PoW that implements the greater the Hash power it has, the greater the process received. Proof-of-Stake can sort out which network nodes that have not been rationed for a long time, so that the node can come first. However, after the node has 1 process, the time will be reset, and the queue will start again. Miners can be determined deterministically by the algorithm based on the age of the node. The higher the age of the node, the higher the chance of getting a turn for the validation process. After getting 1 order, the age time resets back to "0", and will re-enter the initial queue. Like PoW, PoS is also implemented as a system to ward off various digital attacks that may occur, especially Denial of Services and Spamming. Cost is exorbitant to try to carry out attacks on networks that adopt both PoS and PoW systems. PoS is broadly faster and more efficient than PoW systems, because technically, anyone can do mining. PoS also offers a linear scale relative to the percentage of blocks that can be confirmed with its Mining Rig, so the process will be adjusted to the power quota they have.

In the traditional Proof-of-Work (PoW) 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 PoW 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.

In the Proof of Stake model used by Digital Asset Solution Coin, 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 Digital Asset Solution Coin network has remained highly decentralized since its inception: a large number of unique accounts are contributing blocks to the network, and the top five accounts have generated 42% of the total number of blocks.

4.1.1 Digital Asset Solution Coin's Proof of Stake Model

Digital Asset Solution Coin use the system that 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 are located within the block represent the summary of the transaction fees as the result of block generation. No new tokens generated by Digital Asset Solution Coin as a result of block creation. Redistribution of Digital Asset Solution Coin takes place as a result of block generators receiving transaction fees, so the term forging is used instead of mining.

Generation of the subsequent blocks are based on verifiable, unique, and almost-unpredictable information from the previous 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.

There is always a concern on the security of the blockchain in Proof of Stake systems. The following basic principles apply to Digital Asset Solution Coins Proof of Stake algorithm:

- A *cumulative difficulty* value is stored as a parameter in each block, and new level of difficulty are applied to each subsequent block based on the previous blocks value. In case of ambiguity, the network achieves consensus by selecting the block or chain fragment with the highest cumulative difficulty.
- Tokens must be stationary within an account for 1,440 blocks before they can contribute to the block generation process, this mechanism to prevent account holders from moving their stake from one account to another in purpose of manipulating their probability of block generation. Tokens that meet this criterion

contribute to an account's *effective balance*, and this balance is used to determine forging probability.

- Peers allow chain reorganization of no more than 720 blocks behind the current block height. This is aimed to keep an attacker from generating a new chain all the way from the genesis block, any block submitted at a height lower than this threshold is rejected.
- Transactions are deemed safe once they are encoded into a block that is 10 blocks behind the current block height. This is because the extremely low probability of any account taking control of the blockchain by generating its own chain of blocks.

4.2 Tokens

In Digital Asset Solution Coin, tokens are the object of trade not the coin itself. Every transaction related to tokens purchase, sell, transfer, exchange, etc will be subject for certain fee in the form of DAS coins. The minimum transaction fee is staring from 0.05 DAS per transaction. The fee will be adjust based on the transaction type and some other transaction property that are set during the transaction creation.

Tokens can be treated as the digital unit value of real asset that are trade in the marketplace. In which the asset itself could be in the form of property, cars, gold, etc. the marketplace producer who is divining which kind of asset they are trading in and the digital unit value of the asset itself.

4.3 Network Nodes

Any device that is contributing transaction or block data to the network is recognize as a *node* on the Digital Asset Solution Coin network. All device running the Digital Asset Solution Coin software is seen as a node. Nodes are sometimes referred to as "Peers".

There are two types of nodes: *hallmarked* and *normal*. A hallmarked node is a node that is tagged with an encrypted token from an account private key; this token can be decoded to reveal a specific Digital Asset Solution Coin account address and balance that are associated with a node. This made a hallmarked node have greater level of accountability and trust, and so 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 trust within the network and then use that trust for malicious purposes; the barrier to entry (cost of Digital Asset Solution Coin required to build adequate trust) discourages such abuse.

Both transactions and block information can be process and broadcast by each node on the Digital Asset Solution Coin network. Each Blocks received from other nodes are validated, and in cases block validation fails, nodes may be blacklisted temporarily to prevent the propagation of invalid block data.

Each node features a built-in DDOS (Distributed Denial of Services) defense mechanism which restricts the number of network requests from any other node to 30 per second.

4.4 Blocks

The ledger of Digital Asset Solution Coin transactions is built and stored in a linked series of blocks, known as a blockchain. This ledger store permanent record of transactions that are done in the Digital Asset Solution Coin system and establishes the order of transactions based on the occurred timestamp. Every nodes in the Digital Asset Solution Coin network keep a copy of the recorded transactions, and every account that is unlocked on a node (by supplying the account private key) has the ability to generate blocks, as long as at least one incoming transaction to the account has been confirmed 1440 times. Any account that meets these criteria is referred to as an active account.

Each block contains up to 255 transactions, prefaced by a block header that store identifying parameters. Each transaction in a block is represented by common transaction data, specific transaction types also include other transaction detail attachment, and certain transactions may include one or more additional appendices. The maximum block size is 42KB. All blocks contain the following parameters:

- A block version, block height value, and block identifier
- A block timestamp, expressed in seconds since the genesis block
- The ID of the account that generated the block, as well as that accounts public key
- The ID and hash of the previous block the number of transactions stored in the block
- The total amount of Digital Asset Solution Coin represented by transactions and fees in the block
- Transaction data for all transactions included in the block, including their transaction IDs
- The payload length of the block, and the hash value of the block payload
- The block's generation signature
- A signature for the entire block
- The base target value and cumulative difficulty for the block

4.4.1 Block Creation (Forging)

In Digital Asset Solution Coin, to determining which account is eligible to generate a block will be based on Three values, 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

All the active Digital Asset Solution Coin accounts compete by attempting to generate a hash value that is lower than a given base target value in order to win the right to forge (generate) a block. This base target value varies from block to block and is derived from the previous block base target multiplied by the amount of time that was required to generate that block using a formula that ensures 60 seconds average block time.

The calculation is based on the following constants:

- MAX_{RATIO} = 67 - max ratio by which the target is decreased when block time is larger than 60 seconds.
- MIN_{RATIO} = 53 - min ratio by which the target is increased when block time is smaller than 60 seconds.
- γ $(gamma)$ = 0.64

And the following variables:

- S - average block time for the last 3 blocks
- Tp - previous base target
- Tb - calculated base target

The base target is calculated as follows:

- If S>60 ➔ $Tb = Tp * \frac{Min(S,\mathrm{Max}_{Ratio})}{60}$
- Else ➔ $Tb = Tp - Tp * \frac{\gamma*(60-Max(S,\mathrm{Min}_{Ratio}))}{60}$

Target Value

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

$$T = T_b \times S \times B_e$$

where:

T is the new target value

T_b is the base target value

S is the time since the last block, in seconds

B_e 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 x 10^{17} and the minimum target value is one half of the previous blocks base target value.

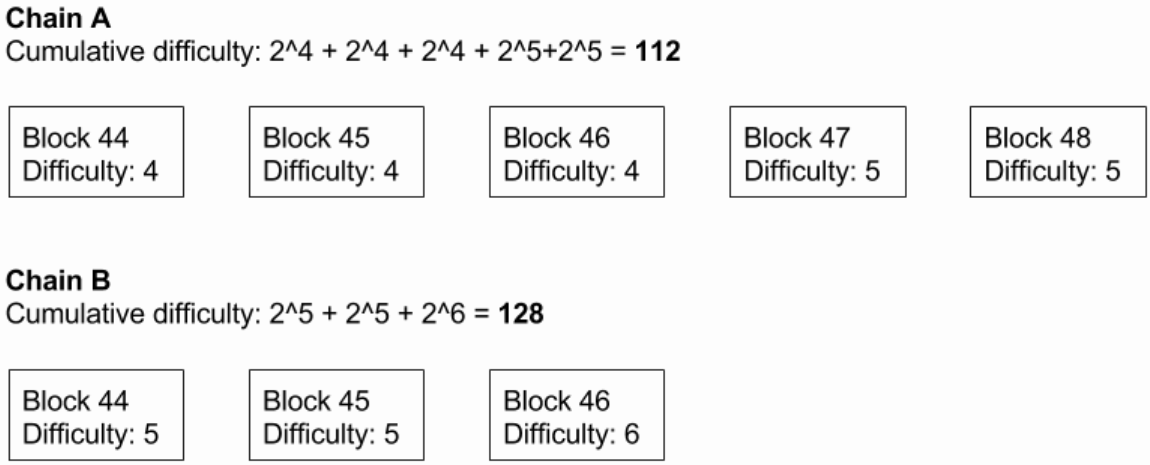
This target value and the base target value are the same for all accounts attempting to forge on top of a specific block. The only account-specific parameter is the effective balance parameter.

Cumulative difficulty

In the most common blockchain implementation, we chose always the "longest" blockchain to be the valid. This must change now that difficulty is introduced. For now, on the "correct" chain is not the "longest" chain, but the chain with the **most cumulative difficulty**. In other words, the correct chain is the chain which required most resources (= hashRate * time) to produce.

To get the cumulative difficulty of a chain we calculate `2^difficulty` for each block and take a sum of all those numbers. We must use the `2^difficulty` as we chose the difficulty to represent the number of zeros that must prefix the hash in binary format. For instance, if we compare the difficulties of 5 and 11, it requires 2^ (11-5) = 2^6 times more work to find a block with latter difficulty.

In the below example, the “Chain B” is the “correct” chain although it has fever blocks:



Only the difficulty of the block matters, not the actual hash (given the hash is valid). For example, if the difficulty is 4 and the block hash is 000000a34c… (= also satisfying the difficulty of 6), only the difficulty of 4 is considered when calculating the cumulative difficulty.

This property is also known as “Nakamoto consensus” and it is one of the most important inventions Satoshi made, when s/he invented Bitcoin. In case of forks, miners must choose on which chain the they decide to put their current resources (= hashRate). As it is in the interest of the miners to produce such block that will be included in the blockchain, the miners are incentivized to eventually to choose the same chain.

The Forging Algorithm

Each block on the chain has a *generation signature* parameter.

An active account digitally signs the generation signature of the previous block with its own public key to participate in the block forging process. In which a 64-byte signature are created, which is then hashed using SHA256. The first 8 bytes of the resulting hash are converted to a number, known as account *hit*.

The hit then compared to the current target value. the next block can be generated if the computed hit is lower than the target. As noted in the target value formula, the target value increases in every second of process. Even if the active accounts on the network is less, block will be successfully generated by one of them because of the target value will

become very large. Therefore, you will be able to calculate the time that needed by any account to forge a block by comparing the account hit value to the target value.

The last point is significant. Since any node can query the effective balance for any active account, iteration through all active accounts in order to determine their individual hit value is possible. This means it is possible to reasonable accuracy predict, which account will be winning the right to forge a block. A balance shifting attack cannot be mounted by moving stake to an account that will generate the next block, since Digital Asset Solution Coin stake must be stationary for 1440 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 Digital Asset Solution Coin forging algorithm helps form the basis for the development and implementation of the Transparent Forging algorithm. Since this algorithm has not yet completely been implemented, and because its implications on the Digital Asset Solution Coin network are significant, it will be outlined in a separate paper.

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

The payload value, generating account, and all 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.

A node which receive a valid block representing a chain with larger cumulative difficulty than its own, will determine the highest common block between its own chain and the chain represented by the new block, then remove its own blocks from the chain down to the common block and undo any side effects of these blocks then build its own chain based on blocks received from other nodes

Balance leasing

To be able to increase effective balance parameter to get bigger chance to wining the right to forge, it is possible for an active account to loan forging power from another

account without giving up control of the tokens associated with the respective account. An account owner may temporarily reduce its accounts effective balance to zero, adding it to the effective balance of another account. The targeted account forging power is increased for a certain number of blocks specified by the original account owner, after which the effective balance is returned to the original account. The account which leased its forging power, does not need to reveal its passphrase in order to participate in forging new blocks. Only the lessee account needs to reveal its passphrase and this account can poses much smaller balance so that in case its passphrase is stolen the loss is minimal. Leasing balance does not affect the functionality of the lessor account except its ability to forge.

4.4.2 Accounts

Brain wallet as part of Digital Asset Solution Coin design: all accounts are stored on the network, with *private keys* for each account address directly derived from each *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 practically eliminates the risk that a typo in account address would result in loss of funds. Account addresses are always prefaced by a *Digital Asset Solution Coin* - prefix, making Digital Asset Solution Coin account addresses easily recognizable and distinguishable from address formats used by other blockchains.

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 accounts *private key*.
2. The private key is encrypted with Curve25519 to derive the accounts *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 Digital Asset Solution Coin, 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

Several different types of balances are available for each Digital Asset Solution Coin account. 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 stay in that account for 1440 blocks. In addition, the Account Leasing feature allows an account's effective balance to be lease to another account for a temporary period. The account effective balance is calculated from the *confirmed balance* by reducing all balance additions during the last 1440 blocks.
- The *guaranteed balance* of an account consists of all tokens that have been stay in an account for 1440 blocks. Unlike the effective balance, this balance cannot be assigned to any other account.
- The *confirmed balance* of an account accounts for all transactions that have had at least one confirmation.
- The *unconfirmed balance* of an account is the one that is displayed in Digital Asset Solution Coin clients. It represents the confirmed balance of an account, minus the tokens involved in unconfirmed, sent transactions or locked by specific transaction types such as Currency Reserve Increase and Shuffling transactions or locked by phased transactions not applied or cancelled yet.
- The *forged balance* of an account shows the total amount of Digital Asset Solution Coin that have been earned as a result of successfully forging blocks.
- Confirmed and unconfirmed asset quantities and currency units are also tracked by each account holdings.

4.4.3 Transactions

To be able to get improve to their state or balance, Digital Asset Solution Coin account must commit transaction. 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 Digital Asset Solution Coin are recirculated back into the network. Every transaction requires a minimum fee. When an Digital Asset Solution Coin account forges a block, all the transaction fees included in that block are awarded to the forging account as a reward. Unlike with other blockchains, minimum transaction fees are enforced by the blockchain therefore transactions which does not specify a fee larger than the minimal fee for this transaction type won't be accepted by nodes.

Transaction Confirmations

All Digital Asset Solution Coin 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 several minutes from the time the transaction is submitted to the network. The default deadline is 1440 minutes (24 hours). A transaction that has been broadcast to the network but has not been included in a block yet 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 until their deadline expire, because they are permanently invalid or malformed, or because they do not meet certain temporary conditions such as sufficient balances, or because blocks are being filled with transactions that have offered to pay higher transaction fees.

Transaction Types

Categorizing Digital Asset Solution Coin transactions into types and subtypes allows for modular growth and development of the Digital Asset Solution Coin protocol without creating dependencies on other base functions. As features are added to the Digital Asset Solution Coin core, new transaction types and subtypes can be added to support them.

Multiple transaction types and associated subtypes are supported by Digital Asset Solution Coin. Each type dictates a given transactions required and optional parameters, as well as its processing method. A complete list of all transaction types and sub types is out of the scope of this document.

Transaction Creation and Processing

The details of creating and processing a Digital Asset Solution Coin transaction are as follows:

1. The sender specifies parameters for the transaction. Types of transactions vary, and the desired type is specified at transaction creation, but several parameters must be specified for all transactions:
    - private key for the sending account
    - specified fee for the transaction
    - 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 the minimum fee for this transaction type; 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:
    1. The public key for the generating account is computed using the supplied secret passphrase
    2. 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 enough funds for the transaction:

0. 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
1. The transaction is signed using the sending account's private key
2. The encrypted transaction data is placed within a message instructing network peers to process the transaction
3. The transaction is broadcast to all peers on the network
4. 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.

4.5 Cryptographic Foundations

Curve25519 algorithm are use on Key exchange in Digital Asset Solution Coin, 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. Digital Asset Solution Coins Java-based implementations were reviewed by DoctorEvil in March 2014.

Message signing in Digital Asset Solution Coin 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.

Both algorithms were chosen for their balance of speed and security for a key size of only 32 bytes.

4.5.1 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:
    - $seed_n$ = SHA256($seed_{n-1}$), where $seed_0$ = SHA256(shared_secret)
3. Calculates N keys:
    - key_n = SHA256(Inv($seed_n$)), where Inv(X) is the inversion of all bits of X
4. Encrypts the plaintext:
    - ciphertext[n] = plaintext[n] XOR key_n

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 Alices step):
    - $seed_n$ = SHA256($seed_{n-1}$), where $seed_0$ = SHA256(shared_secret)
3. Calculates N keys (this is identical to Alices step):
    - key_n = SHA256(Inv($seed_n$)), where Inv(X) is the inversion of all bits of X
4. Decrypts the ciphertext:
    - plaintext[n] = ciphertext[n] XOR key_n

5. Core Features

5.1 Advanced JavaScript client

A user-friendly client application is built in Digital Asset Solution Coin core software distribution and accessible through a local web browser. The client provides full support for all core Digital Asset Solution Coin features, implemented such that users' private keys are never exposed to the network. It also includes an advanced administrative interface and built-in Javadoc documentation for Digital Asset Solution Coins Low-level Applications Programming Interface.

5.2 Agile architecture

Cryptocurrencies were primarily designed as payment systems. Digital Asset Solution Coin recognizes that decentralized blockchains could be leveraged to broader range of applications and services but is not prescriptive about what those services should be or how they should be built. By design, Digital Asset Solution Coin strips away unnecessary complexity in its core, leaving only the most successful components of its predecessors intact. As a result, Digital Asset Solution Coin functions like a low-level, foundational protocol: it defines the interfaces and operations required to operate a lightweight blockchain, a decentralized communication system, and a rapid transaction processing framework, allowing higher-order components to build on those features.

Digital Asset Solution Coin make simple adjustments to account balances based on every Transactions instead of tracing sets of input or output credits. The core software does not support any form of scripting language. Digital Asset Solution Coin creates a foundation that does not limit the ways in which those transaction types can be used and does not create significant overhead for using them, by providing a set of basic, flexible transaction types that can quickly and easily be processed. This flexibility is further amplified by Digital Asset Solution Coins low resource and energy requirements, and its highly readable, highly organized object-oriented source.

5.3 Basic Payments

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

5.4 Alias System

The Digital Asset Solution Coin Alias System allows any string of text to be permanently associated with a specific Digital Asset Solution Coin account. Since its inception, a convention for the format of these strings, using JSON notation, has been formalized. As a result, an alias can currently be human-friendly text alias for an account address or a Uniform Resource Identifier (URI).

The ability to store any URI on the Digital Asset Solution Coin blockchain enables the creation of any number of decentralized services that rely on small, persistent strings of text, such as a distributed Domain Name Server (DNS) system.

5.5 Arbitrary Messages

By using the Arbitrary Messages feature, Digital Asset Solution Coin blockchain able to store strings of data up to 1000 bytes in length, and these strings may optionally be AES-encrypted. 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 several next-generation features.

At the basic level, the system can transmit human-readable messages between accounts, creating a decentralized chat system. However, advanced applications can use this feature to store structured data, such as JSON objects, that can be used to trigger or facilitate services built on top of Digital Asset Solution Coin. The most notable current implementation is the Digital Asset Solution Coin Multi gateway (MGW), part of the Digital Asset Solution Coin Services layer, which employs the Arbitrary Messaging system to drive a nearly-trustless method for automatically transforming Bitcoin, Litecoin, and other cryptocurrencies into Digital Asset Solution Coin assets (based on the colored coins concept) that can be traded, bought, and sold on the fully-decentralized asset exchange.

5.6 Asset Exchange

An entire class of Digital Asset Solution Coin transactions is used to implement a fully decentralized and automated asset exchange that operates on the Digital Asset Solution

Coin blockchain. Using the colored coins concept, Digital Asset Solution Coin assets may be issued and tracked on the Digital Asset Solution Coin 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 Digital Asset Solution Coin Asset Exchange with other features such as the Arbitrary Messaging System, value-added services can be created. Most notably, another feature of the Digital Asset Solution Coin Services layer is a system for the automated calculation and disbursement of dividends based on the performance of existing Digital Asset Solution Coin assets.

5.7 Digital Goods Store

The Digital Asset Solution Coin Digital Goods store gives account owners the ability to list assets for sale in an open, decentralized marketplace. 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.

5.8 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, Digital Asset Solution Coin is extremely well suited for use on small, low-power, low-resource devices. Android and iPhone applications are currently in development, and the Digital Asset Solution Coin software has been ported to low-powered ARM devices such as the RaspberryPi and CubieTruck platforms.

The ability to implement Digital Asset Solution Coin on low-powered, always-connected devices such as smartphones allows us to envision a scenario where the majority of the Digital Asset Solution Coin 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.

6. Concerns

6.1 Proof of Stake Attacks

6.1.1 Nothing at Stake

Nothing-at-stake is a theoretical security issue in proof-of-stake consensus systems in which validators have a financial incentive to mine on every fork of the blockchain that

takes place, which is disruptive to consensus and potentially makes the system more vulnerable to attacks.

While this attack is theoretically possible, it is currently not practical. The Digital Asset Solution Coin network does not experience long blockchain forks, and the low block reward does not provide a strong profit incentive; further, compromising network security and trust for the sake of such small gains would make any victory pyrrhic.

As part of Digital Asset Solution Coins development roadmap, a feature called Economic Clustering will provide further protection against attacks of this nature by forcing transactions to include hashes of previous blocks, and by grouping nodes into clusters that can detect unusual behavior on the network and impose penalties (in the form of temporary loss of the ability to forge).

6.1.2 History Attack

In a history attack, someone acquires a large number of tokens, sells them, and then attempts to create a successful fork from just before the time when their tokens were sold or traded. If the attack fails, the attempt costs nothing because the tokens have already been sold or traded; if the attack succeeds, the attacker gets their tokens back. Extreme forms of this attack involve obtaining the private keys from old accounts and using them to build a successful chain right from the genesis block.

In Digital Asset Solution Coin, the basic history attack generally fails because all stake must be stationary for 1440 blocks before it can be used for forging; moreover, the effective balance of the account that generates each block is verified as part of block validation. The extreme form of this attack generally fails because the Digital Asset Solution Coin blockchain cannot be re-organized more than 720 blocks behind the current block height. This limits the time frame in which a bad actor could mount this form of attack.

6.2 Transaction Fees

The cost of minimum transactions fees, known as fiat, will increases as the value of Digital Asset Solution Coin increases. Plans are underway to reduce the minimum fee, scaled according to transaction byte-size, in order for micro-transactions to be practical.

7. Bitcoin Problems Addressed by Digital Asset Solution Coin

Digital Asset Solution Coin was created as a cryptocurrency 2.0 response to Bitcoin. Digital Asset Solution Coin adopts features that have proved to work well in Bitcoin, and addresses aspects that are cause for concern. This appendix addresses issues with the Bitcoin protocol and network that are mitigated by Digital Asset Solution Coin technology.

7.1 Blockchain Size

The Bitcoin blockchain is the complete sequential collection of generated data blocks containing the electronic ledger book for all Bitcoin transactions occurring since its launch in January 2009. Four years later in January 2013, the size of the Bitcoin blockchain stood at 4 gigabytes (GB) about the amount of data required to store a two-hour movie on a DVD disk. Eighteen months later, in July 2014, the size of the Bitcoin blockchain had swelled by almost a factor of five to 19 gigabytes (GB). The Bitcoin blockchain is undergoing exponential growth and modifications to the original Bitcoin protocol will be required to deal with it.

7.1.1 Digital Asset Solution Coin Solutions

Digital Asset Solution Coin block size is currently capped at 32KB. Since its inception, almost 181,000 blocks have been generated and the blockchain takes up 390MB of space. In the future, Digital Asset Solution Coin will implement a Blockchain Pruning feature (still under discussion) that will reduce blockchain size by selectively removing information on permanent blocks, and by deleting other non-persistent data, such as Arbitrary Messages.

7.2 Transactions per Day

In late 2019, the number of transactions being processed on the Bitcoin network was peaking at 70,000 per day, which is about 0.8 transactions per second (tps). The current Bitcoin standard block size of one megabyte, generated every ten minutes (on average) by full node clients, limits the maximum capacity of the current Bitcoin network to a about 7 tps. Compare this with the VISA network's capacity to handle 10,000 tps and you will see that Bitcoin cannot compete as it exists today.

Increasing public use of the Bitcoin system will cause Bitcoin to soon hit its transaction-per-day limit and halt further growth. To forestall this, Bitcoin software developers are working on the creation of thin clients that employ simplified payment verification (SPV). To handle greater throughput in the same 10-minute-average time, SPV thin clients will not perform a full security check on the larger blocks they process. They will instead

examine multiple hashed blockchains from competing miners and assume that the blockchain version generated by the majority of miners is correct. In the words of Bitcoins Mike Hearn, instead of verifying the entire contents, [SPV] just trusts that the majority of miners are honest…. As long as the majority is honest, [SPV] works… [However], the full node does give you better security. If you're running an online shop for example, it makes sense to run a full node.

7.2.1 Digital Asset Solution Coin Solutions

In its current state, the Digital Asset Solution Coin network can process up to 367,200 transactions per day more than nine times Bitcoins current peak values. The planned implementation of Transparent Forging will allow for near instant transaction processing, drastically increasing this limit.

7.3 Transaction Confirmation Time

Transaction confirmation times for Bitcoin ranged from 5 to 10 minutes for most of 2013. After the late 2013 announcement that Chinese banks would not be allowed to process Bitcoins, the average Bitcoin transaction time significantly increased to 8 to 13 minutes, with occasional peaks of 19 minutes. Confirmation times have since resettled in the 8 to 10-minute range. Nonetheless, since multiple verifications are required to finalize a Bitcoin transaction (six confirmations are generally preferred), one hour can easily pass before a sale of assets paid for by Bitcoin is complete.

7.3.1 Digital Asset Solution Coin Solutions

The average block generation time for Digital Asset Solution Coin has historically been shown to be about 60 seconds, putting the average transaction processing time at the same value. Transactions are deemed safe after ten confirmations, meaning that transactions are permanent in less than 30 minutes.

The implementation of Transparent Forging will allow for nearly instant transactions, which will further reduce this time.

7.4 Centralization Concerns

The increasing difficulty and combined network hash rate for Bitcoin has created a high barrier to entry for newcomers, and diminished returns for existing mining rigs. The block reward incentive employed by Bitcoin has driven the creation of large, single-owner installations of dedicated mining hardware, as well as the reliance on a small set of large mining pools. This has resulted in a centralization effect, where large amounts of mining

power are concentrated in the control of a decreasing number of people. Not only does this create the kind of power structure that Bitcoin was designed to circumvent, but it also presents the real possibility that a single mining operation or pool could amass 51% of the network's total mining power and execute a 51% attack. Attacks requiring as little as 25% of total network hashing power also exist.

7.4.1 Digital Asset Solution Coin Solutions

The incentives provided by Digital Asset Solution Coins Proof of Stake algorithm provide a low Return on Investment of approximately 0.1%. Since no new coins are generated with each block, there is no additional mining reward that incentivizes combining efforts to generate blocks. Data shows that the Digital Asset Solution Coin network has remained highly decentralized since its inception: a large (and growing) number of unique accounts are contributing blocks to the network, and the top five accounts have generated 35% of the total number of blocks.

7.5 Proof of Work's Resource Costs

Confirming transactions for existing Bitcoins, and creating new Bitcoins to go into circulation, requires enormous background computing power that must operate continuously. This computing power is provided by so-called mining rigs operated by miners. Bitcoin miners compete among themselves to add the next transaction block to the overall Bitcoin blockchain. This is done by hashing - bundling all Bitcoin transactions occurring over the past ten minutes and trying to encrypt them into a block of data that also coincidentally has a certain number of consecutive zeros in it. Most trial blocks generated by a miner's hashing effort don't have this target number of zeros, so they make a slight change and try again. A billion attempts to find this winning block is called a gig hash, with a mining rig being rated by how many gig hashes it can perform in a second, denoted by *GH/sec*. A winning miner who is first to generate the next needle-in-a-haystack, cryptographically correct Bitcoin block currently receives a reward of 25 newly-mined Bitcoins - a reward worth, at the time of this writing, around $15,750USD. This competition among miners, with its hefty reward, repeats itself over and over and over every ten minutes or so. By early 2019 over 3500 bitcoins per day are generated, worth around $2.2 million US dollars per day.

With so much money at stake, miners have supported a blistering arms race in mining rig technology to better their odds of winning. Originally Bitcoins were mined using the central processing unit (CPU) of a typical desktop computer. Then the specialized graphics processing unit (GPU) chips in high-end video cards were used to increase speeds. Field programmable gate array (FPGA) chips were pressed into service next, followed by mining

rigs specialized application specific integrated circuits (ASIC) chips. ASIC technology is the top of the line for Bitcoin miners, but the arms race continues with various generations of ASIC chips now coming into service. The current generation of ASIC chips are the so-called 28nm units, based on the size of their microscopic transistors in nanometers. These are due to be replaced by 20nm ASIC units by late-2014. An example of an upcoming state-of-the-art mining rig would be a Butterfly Labs Monarch 28nm ASIC card, which is to provide 600GH/sec for an electricity consumption of 350 watts and a price of $2200USD.

The mining rig infrastructure currently in place to support ongoing Bitcoin operations is astounding. Bitcoin ASICs are like autistic savants - they can do only the Bitcoin block calculation and nothing more, but they can do that one calculation at supercomputer speeds. In November 2013, Forbes magazine ran an article entitled, Global Bitcoin Computing Power Now 256 Times Faster Than Top 500 Supercomputers, Combined. In mid-January 2014, statistics maintained at blockchain.info showed that ongoing support of Bitcoin operations required a continuous hash rate of around 18 million GH/sec. For one day, that much hashing power produced 1.5 trillion trial blocks that were generated and rejected by Bitcoin miners looking for one the magic 144 blocks that would let them $2.2 million USD. Almost all Bitcoin computations do not go towards curing cancer by modeling DNA or to searching for radio signals from E.T.; instead, they are totally wasted computations.

The power and cost involved in this wasteful background mining support of Bitcoin is enormous. If all Bitcoin mining rigs had Monarch levels of capability as described above - which they will not, until they are upgraded - they would represent a pool of 30,000 machines costing over $63 million USD and consuming over 10 megawatts of continuous power while running up an electricity bill of over $3.5 million USD per day. The real numbers are significantly higher for the current, less-efficient mining rig pool of machines actually supporting Bitcoin today. And these numbers are currently headed upward in an exponential growth curve as Bitcoin marches from its current one transaction per second to its current maximum of seven transactions per second.

7.5.1 Digital Asset Solution Coin Solutions

Analysis of the cost and energy efficiency of the Digital Asset Solution Coin network shows that the entire Digital Asset Solution Coin ecosystem can be maintained for about $60,000USD per year, which is currently almost 2,200 times less expensive than the cost of running the Bitcoin network.

7.6 Proof of Work's Resource Costs Pertaining to Coin holders

In addition to massive electrical costs, there is a hidden fee for simply holding Bitcoins. For each block found, the entity that generates the block receives a stipend. At the time of writing, this stipend is 25 BTC, producing 10% inflation in the total Bitcoin supply this year alone. For each $1000USD worth of Bitcoin someone owns, that person is paying $100USD per Bitcoin this year to pay miners for keeping the network secure.

7.6.1 Digital Asset Solution Coin Solution

Since the complete supply of Digital Asset Solution Coins 1 billion coins was created with the genesis block, there is no inflation in Digital Asset Solution Coin. Deflationary pressures are likely to affect Digital Asset Solution Coin in the future, and a planned feature called Ant deflation (design in progress) will address that problem.

8. Application and Future works

8.1 Application

Digital Asset Solution Coin could be implemented in such business model such as Financial Service and Digital Payment system

8.1.1 Asset Investment

Digital Asset Solution Coin designed for develop a stable coin environment. Every asset could be trade on top of DAS platform. The token trade instead of the coin, will make the coin value stable.

8.1.2 Digital Exchange

Digital Asset Solution Coin provide the flexibility to exchange to IDR currency and reverse. Beside to manage the liquidity of the investment, this also open opportunity for everyone to manage the fund in other form such as coin, rather than saving it in the bank.

8.2 Future works

Currently DAS coin can be exchanged directly to IDR currency, in the future, DAS will be developed more function to be able to exchange with other currencies including other crypto currency such as BTC, etc