DasCoin™

DasCoin:
A Convertible Store of Value Unit within a Digital Asset System

Michael Mathias

DRAFT

January 15th, 2017

Abstract

The DasCoin Blockchain establishes a system for securely creating and exchanging cryptographic assets. The DasCoin Ecosystem is structured in a manner that delivers greater security, scalability, efficiency, and performance. At the core of this system is DasCoin, a hybrid cryptocurrency that combines the best qualities of decentralized cryptocurrencies with the best aspects of centralized currencies – and eliminates their weaknesses. DasCoin serves as the convertible store of value unit at the center of the digital asset system. The value of DasCoin is supported by a range of innovative solutions that create real-world utility for individuals and businesses and create financial institutions, cooperatives and merchants.

Introduction

Technology-based money has now become a reality and is poised to grow for generations to come. Bitcoin has been the pioneer in this emerging segment, and has demonstrated how it was possible to digitally format a money system. Bitcoin has experienced a significant degree of success in the eight years its been in existence. Since that time, other cryptocurrencies have followed but have made little impact on the market.

There are severe weaknesses to the two dominant models in the cryptocurrency industry. Bitcoin's proof-of-work model is a brutally inefficient system and its decentralized structure leads to serious governance issues. Proof of stake coins are all pre-distributed and have very little validity (due to the "nothing at stake" problem).

DasCoin offers a hybrid alternative: a private, permissioned blockchain architecture has been incorporated due to its enhanced security, inherent efficiency and ability to scale more easily. The system builds on this foundation by authenticating all of its users in accordance with banking-standard KYC (Know Your Client) requirements and incorporating a powerful marketing system into the overall value proposition. The result is system of digital value that is capable of world-class performance and that is also poised for rapid global adoption by the mass market.

Key Design Features

Proof of Value Distribution

Anyone that is distributed DasCoins has presented the system with a form of recognized value (either Bitcoin or euros). Developers are no pre-mining or pre-distributing coins to themselves.

Proof of License Consensus

DasCoin is built as a licensing system not as a mining apparatus. Consensus is reached through an algorithm which defines randomly what licensed node is going to make the next block.

Fixed Supply of DasCoins

2 to the 33rd, about 8.5 billion units (distributed over an undefined period – dependent on internal dynamics of the system -- that is currently approximated at 12 years)

Authentication

Authentication through licenses and KYC (the banking standard defined as Know Your Customer) processes.

Conversion unit within the system

From fiat currency or Bitcoin to 'Cycles' and then from 'Cycles' to 'DasCoin'.

Ecosystem

Distributed ecosystem of digital value consisting of digital wallets and products around it including trading exchange functions, payment solutions, authentication.

Marketing System

A marketing-based system to support the development of an affinity group around DasCoin.

Hybrid Features

DasCoin combines features of centralized and decentralized approaches with the view of maximizing benefits to the users. These include:

- Centralized emissions of coins.
- Permissioned blockchain that will be independently verified.
- Distributed network, decentralized ecosystem – once a coin is issued, it exists in a digital wallet and is only available to that user. No other company or authority can confiscate or seize that.
- Authenticated userbase through KYC process to support trust among participants.
- Privacy with transparency in the way transactions are made and recorded.
- Full compliance with KYC regulation: DasCoin wants to to be compliant with major jurisdictions and is keen to engage with regulators.
- Instant transactions with a transaction validation speed set at 6 seconds.

Key Objectives

DasCoin has been created with the following objectives in mind:

- Capital appreciation: there is a clear objective for DasCoin to become a store of value. As the digital value in the ecosystem grows, so will the value of the unit.
- Liquidity
- Utility, including a payment system
- Security

Another objective of DasCoin is to use the infrastructure of a cryptocurrency to build an effective network of trust, enabling all participants and stake holders to share a common goal of increasing the value of the network and cultivating its growth. The network will achieve this by:

1. Granting trust to certain roles (such as the DasCoin Board and chain authorities) to perform chain management in order to maximize the efficiency and utility of the network.
2. Programmatically ensure that each trusted role is well defined and does not overstep the boundaries of its authority.
3. Provide an incentive to behaving within the common interest of the network, and make sure that any misbehaving authority is shut off from the network and liable to be punished for breaking the rules.

In this way, the DasCoin system provides iterations of innovation, enabling necessary updates to match conditions both within the network and regarding the world at large. Ultimately, the system will create a set of agreed upon rules for creating and transmitting value and enforcing it through the Blockchain software.

In a sentence: LAW is CODE.

Definitions

Private Key
A 32-byte number generated through a sufficiently random method of generation.

Public Key
A point on the secp256k1 elliptic curve.

DasCoin Ecosystem
A digital asset system capable of securely creating, transferring, and accounting for a variety of cryptographic assets. The ecosystem features blockchain, wallet, network and exchange functionality.

DasNet
The Vault Account is an individual identity of a person who uses the DasCoin Blockchain. This account holds the licensing information obtained by the person.

DasCoin Blockchain
A private, permissioned blockchain architecture that features enhanced security, inherent efficiency and ability to scvale more easily.

Vault Account

A cryptographic asset defined in the DasCoin Blockchain. Cycles represent resources that were introduced to the network.

DasCoin
The Vault Account is an individual identity of a person or business entity who has been authenticated to use the DasCoin Blockchain. This account holds the licensing information obtained by the person or business entity.

License
A cryptographic certificate that enables an account to participate on the DasCoin Blockchain.

Cycles
A cryptographic asset defined in the DasCoin Blockchain. Cycles represent stored capacity within DasNet and can either be used for network services or submitted for DasCoins.

DasCoin
A convertible store of value unit that is at the center of a digital asset system. DasCoins are produced and distributed when Cycles are submitted to DasNet.

Frequency
The conversion factor that determines the amount of Cycles that will yield a DasCoin in the minting process.

DasCoin Minting
The process of producing and distributing DasCoins in exchange for submitted Cycles.

DasCoin Minting Queue
The line up of users who have submitted their Cycles to redeem for DasCoin. The queue operates on a First-In-First-Out basis.

DasCoin Interval
The duration between DasCoin Minting Distributions.

DasCoin Distribution Rate
The number of DasCoins that will be distributed during the elapsing of a DasCoin Interval.

WebEuro
A cryptographic asset defined in the DasCoin Blockchain that represents the euro denomination.

Transaction Ledger

OPERATIONS

Operations are the foundation for constructing transactions.

They are defined using the C++ programming language which allows for the creation of dynamic and expansive activities to take place over the Blockchain. Operations describe the potential logic that a person or the nodes can perform. These can be added and updated in real time upon approval of software updates. This means that it is possible to provide customized digital contracts that are reinforced programmatically by the Blockchain and its node network.

TRANSACTIONS

Transactions are the summary of operations intended by some activity.

Once the set of operations are defined, the participant of the transaction must appropriately sign with their private key the corresponding operation. These will be checked and verified and include an expiration date, a block number, and a reference to the block number's hash. Once all required fields are filled and each operation is signed by the respective keys only then can it be successfully included in a block and written to the history of the Blockchain Ledger.

BLOCKS

A Block is a group of transactions that updates the state of the Blockchain Ledger

Blocks are the foundational element to the Blockchain. Each block is made by an authoritative entity called a Master Node and each block is cryptographically linked to the previous block. This cryptographic continuity ensures the integrity of the balances that are being modified on the ledger. Replaying the sequence of blocks will reveal the current existing state, and the application of blocks sequentially means that there cannot be any inconsistencies between any balances of the accounts residing on the Blockchain.

Blocks are immutable because they contain a time stamp, have the signature of the Master Node that approved of it, and will become linked to future blocks. This means that when people make transactions they are irreversible and they cannot be modified without completely affecting all other aspects of the system. Any invalid signature will be refused therefore, no one can easily mutate or modify the existing history of the Blockchain.

Decentralized Consensus

MASTER NODES

The role of the Master Node is to aggregate transactions with the intention to produce Blocks. Only Master Nodes have the authority to write transactions into the Blockchain ledger history. Each Master Node is aware of the other and they must have been voted in by the governing system. Master Nodes are novel in that their authority is represented with cryptographic keys. This means that each Master Node must have registered its Public Key and will sign with its Private Key during the time of Block Production. Therefore, it is possible to hold any one particular Master Node accountable for its actions.

LEDGER NODES

Ledger Nodes are non-authoritative maintainers of the DasCoin Blockchain. In other words, Ledger Nodes do not produce blocks; yet they aggregate transactions and pass them to the Master Nodes for Block inclusion. Ledger Nodes are able to verify transactions and therefore they are useful for increasing the foot print of the DasCoin Consensus Network and permit connectivity to reach farther without requiring the need to assign authority to node. Transaction propagation is accelerated because of Ledger Nodes.

BLOCK PRODUCTION

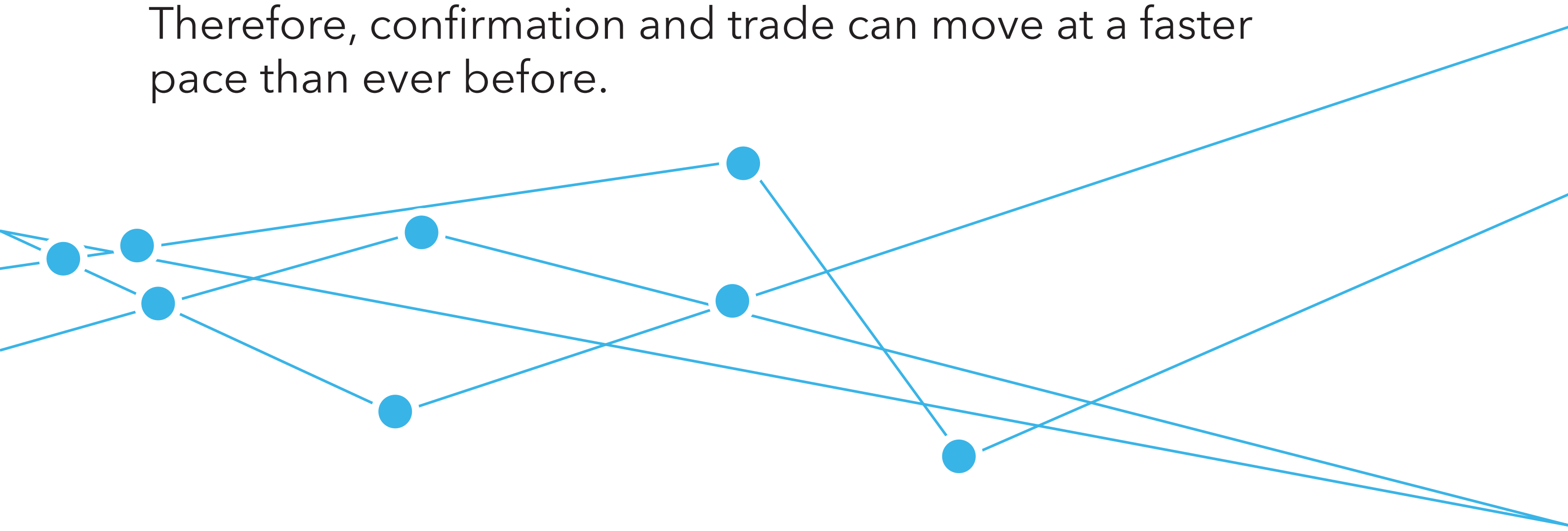
Each Master Node is given a fair chance to produce a block. Until each Master Node has participated in producing a Block, their order is randomized again. This prevents any one Master Node from dominating block production which could potentially lead to network instability and transactions from not being confirmed in the ledger. Every 6 seconds, another Master Node is selected and is responsible for producing the block for that index. If they fail to produce a block, then the next Master Node will take over in producing the block for the same index.

SOFTWARE UPDATES (HARD FORKS)

Over time updates in the form of improvements and feature implementations will need to be incorporated into the Blockchain software. Therefore, it is made possible to upgrade the technology even while it is already operating. At least 51% of Master Nodes must approve of a software change in order to incorporate it into the overall utility of the network. However, this allows the DasCoin stakeholders to incorporate feature requests and for developers to optimize the performance of the software.

High Speed Node Network

The DasCoin Ecosystem exposes new power and possibility as a Blockchain and Cryptocurrency since Master Nodes need to only store their private signing key and be authenticated with the rest of the network. This means that the Master Nodes need only to validate transactions against the history before producing a block. The sooner the Node can verify all signatures and balances the sooner it can produce a block and move on. Therefore, confirmation and trade can move at a faster pace than ever before.



The quality of hardware and network configuration which enables better capture of transactions from around the world greatly improves reliability and stability for commerce. Because of these advancements the network can confirm transactions and permit balance updates in as little at 6 (six) seconds. Optimization to the Blockchain software will greatly reduce the time required to confirm and propagate blocks.

Middleware

DasNet is a sophisticated network that is intended for Blockchain hosting and global access to transaction capture and verification. For this reason, DasCoin is hosted on a network architecture that is a state-of-the-art standard that is specifically designed for securing a reliable network and scaling around the world.

Middleware

Hardware Infrastructure

DasNet is exclusively hosted in data centers based on a criteria that access to the server rack is physically secured. They are compatibly connected to other data centers around the world over leased direct lines affording reliable and highly connected bandwidth. This approach gives DasNet control of the entire path between data centers and permits prevention of man-in-the-middle attacks as well as Denial of Service and Distributed Denial of Service attacks among the nodes that maintain the Blockchain and its connectivity to service.

DasNet has two additional layers for handling transaction capture and network connectivity in addition to the core infrastructure features mentioned previously. The server configuration involves state-of-the-art quality components and protection for high-end threat prevention and hardware based firewall solutions that are commonly utilized by banks and other highly secure environments. In addition, DasNet is hosted on powerful servers that operate with 44 cores per server which provides an efficient space and power consumption to scale into very high traffic and utilization globally.

Software Infrastructure

Connectivity to the DasCoin Blockchain also rides on a software level service that enables access to the core services while keeping its high isolation and security. These services offer and support core service load balancing as well as redundancy and ease to scale as network resources may be needed with a growing network utilization.

Access to the DasCoin Blockchain requires configuration for authorized parties to transmit relevant information from the Blockchain and its internal operations. It also undergoes 24/7 monitoring and support in order to maintain both external services and the key parameters of the core services. Each of these components and services enable a high-speed block production rate as well as maintenance of the integrity of its operation. The immutably and cryptographic connection between all activities defends the principles of the DasCoin Blockchain and DasNet.

Licensing System On-boarding

In order for some person or entity to become an active participant in the DasNet, they must obtain a license. The Blockchain software allows for a service to be authorized to connect and register new accounts. Depending upon how much Resources (or Value) was contributed will determine the level of the Licenses which determines the scale at which a person or entity can participate in the network.

Once a license is purchased, the recipient must register a Wallet Account and a Vault Account in order to redeem the license and take full advantage of the software.

Licensing System On-boarding

VAULT ACCOUNTS

Vault Accounts hold personal information of the user and these are the accounts that are actually receiving licenses. The account is registered to the DasCoin Blockchain and the license is assigned by the License Issuing Authority. Once a license is granted, the Vault Account will receive Cycles and any future commissions from marketing will be deposited directly to the Vault Account using the cryptographic representation of euro currency. Vault Accounts have quantity restrictions depending on license level and authentication level. For a Vault Account to be in use, it must be connected with a Wallet Account. The Vault Account is also the account where Cycles can be submitted to the DasCoin Minting Queue.

WALLET ACCOUNTS

Wallet Accounts provide free trade services to the participants of the DasNet. This account can accept transfers from the Vault Account and perform Wire Out transactions as well as transfer funds to other Wallet and Vault Accounts on the network.

TETHERING

When someone is activating their license with the Vault Account they must have a Wallet Account. These two accounts become tethered and are then related. A Wallet Account can be connected to as many Vault Accounts as a user is willing to share. The tethering process involves a signature from both the Vault and Wallet Account simultaneously in order to perform a successful tethering transaction.

KYC & AML
(KNOW YOU CUSTOMER & ANTI MONEY LAUNDERING)

Each Vault Account must be licensed in order for a person or entity to be able to use the DasNet. The license level also determines the level of amounts a Vault Account can transfer to the Wallet Account per day. A higher level license enables the person or entity to increase their level of verification and therefore increases their access to more capacity within the system and higher withdrawal privileges. This way the DasCoin Blockchain and DasNet can be fully compliant with global regulations that require people to be identified to be in good standing before engaging in commerce with other partners of the DasNet. This gives a higher level of integrity amongst participants and a greater degree of adoption by most jurisdictions in the world.

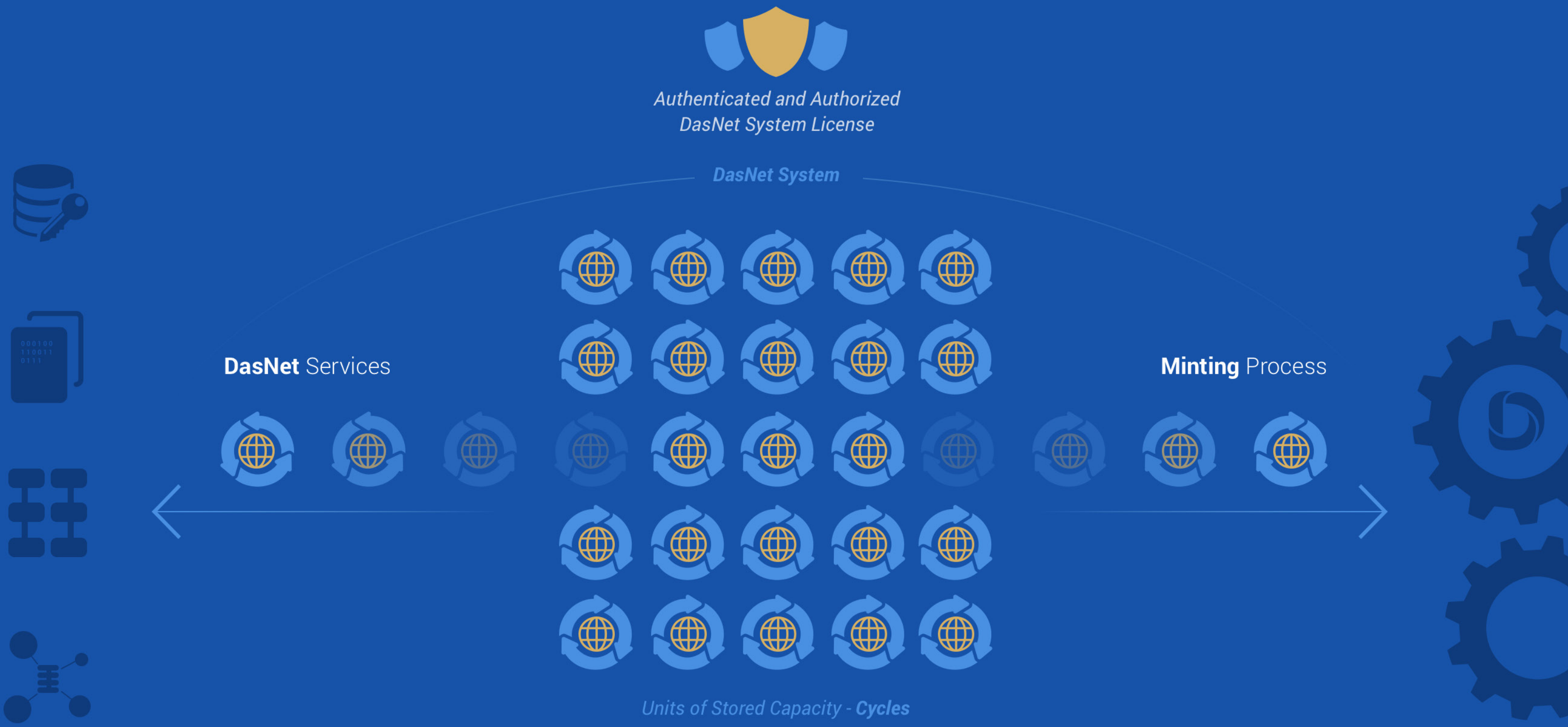
WebWallet™

WebWallet

WebWallet is an access point in order to provide a user-friendly way to gain access to DasCoin and the other crypto assets that are accessible on the DasCoin Blockchain. This crypto wallet is in the form of a website. When a person makes an account through the wallet, the ECDSA keys are generated on the client's browser. The client encrypts their key pair with AES 256 and sends the encrypted key pair to the server's database. In the future, the person can access their account and retrieve their encrypted keys. Only a correct password will unlock and permit use of the keys.

Generating the keys is handled by presenting the participant with 12 randomly generated words which are used as entropy for key creation. These 12 words can be used to restore access in case the AES 256 password is forgotten since the password to the stored keys on the wallet server cannot be recovered. This way the person can always make a new wallet and import their 12-word mnemonic.

DasCoin Minting



The process of producing and distributing new DasCoins is known as Minting. This allows a person or entity to store value in the form of DasCoins. In order to obtain DasCoins people can submit Cycels to the network and then be assigned a place in the DasCoin Minting Queue. On a First-In-First-Out basis, DasCoins are awarded to the account that is next in line of the distribution queue. Each DasCoin Distribution Interval a specific amount of DasCoins are distributed to participants in the queue until the amount of DasCoins to be distributed have been utilized until the next DasCoin Distribution Interval.

The amount of DasCoins to be received is regulated by a factor called Frequency in such a way that the amount of Cycles submitted divided by the Frequency equals the number of DasCoins that should be awarded to that person. The account is deducted Cycles at the time of submission and at the time of distribution the DasCoins are automatically transferred to the account by the blockchain software.

The distribution is done in accordance with the following algorithm:

```
While amount_to_distribute > 0 and not queue.empty() do
element = queue.front()
If element.frequency_lock exists then
      Dascoin = element.cycles/element.frequency_lock
Else
      Dascoin = element.cycles/global_frequecy
Endif
If amount_to_distribute >= dascoin then
      queue.pop_front()
      issue dascoin to element.account_id
      amount_to_distribute = amount_to_distribute - dascoin
Else
      If element.frequency_lock_exists Then
            cycles_to_remove = amount_to_distribute * element.
frequency_lock
      Else
            cycles_to_remove = amount_to_distribute * global_frequency
      Endif
      issue amount_to_distribute to element.account_id
      element.cycles = element.cycles - cycles_to_remove
      queue.update_front(element)
Endif
Loop
```

Periodically all Cycle balances will experience an Upgrade and the balances in the accounts will double. If Cycles are already in the DasCoin Minting Queue these will be unaffected.

Blockchained Internal Exchange

The DasCoin Blockchain also incorporates a decentralized exchange that trades, settles, and clears over the Blockchain autonomously. This way people do not have to choose to transfer their currency to custodial accounts in centralized exchanges in order to conduct some forms of trade. For example, WebEuros are also cryptographic assets in a similar form as DasCoins and therefore, without withdrawing from your wallet the holder is able to trade DasCoins for euro denominations directly on the blockchain.

Because of this the levels of theft from third-parties is greatly reduced and the friction for trade and conversion into national fiat currencies is simple and direct. Using a Wire Out feature a licensed user of the DasCoin Blockchain could withdraw Euros directly to their bank account.

Governance of the Network

DasCoin governance consists of a member-owned association comprised of clients that hold a non-trivial amount of DasCoin. All members of this association may have a say in the running of the network by voting in regular elections for the DasCoin Board, by being active in proposing members for the DasCoin board and by participating in future referendums on critical issues. Unlike a stake based system, the votes are democratic, meaning each holder of DasCoin shall have a single vote.

THE DASCOIN BOARD

The DasCoin Blockchain enables a decentralized governing board to regulate the parameters of the network. The board will be comprised of members elected by stakeholders. The role of the board is to:

1. Propose and modify chain parameters to support the normal functioning and growth of the network.
2. Delegate certain executive roles to certain chain executives (such as issuing licenses and authenticating said licenses).
3. To act as a check on the power of said executives by having the ability to shut them off from the network.

The board itself has no control on the state of the database or the construction of the blockchain and is programmatically prevented from making any changes to it. The network itself manages and maintains the state and the transaction ledger - the only way to make any undesired change is to subvert the majority of master nodes.

Governance of the Network

CHAIN AUTHORITIES

Chain authority roles exist to handle smooth inputs to the Blockchain of user data that exists outside of the system. The problem with fully decentralized systems is the fact that they cannot have reliable inputs: for example Bitcoin is created internally in the Bitcoin blockchain and is merely transferred around. In order for Proof of Value to work, there must be certainty that the user is actually bringing in value to the network. Value cannot exist without an independent observer - and so the only way to verify that the user has submitted value to the system is to maintain an impartial observer.

Each authority role is set up in such a way that:

1. Propose and modify chain parameters to support the normal functioning and growth of the network.
2. The actions of the authority are checked by a separate authentication authority and there are programed measures to assure there is minimal chance of collusion.
3. There are incentives to perform in the best interest of the network.
4. Any malicious action by the chain authority is transparent, and will lead to that account be marked as untrustworthy, shut off from the network and penalized.

The board itself has no control on the state of the database or the construction of the blockchain and is programmatically prevented from making any changes to it. The network itself manages and maintains the state and the transaction ledger - the only way to make any undesired change is to subvert the majority of master nodes.

Global Parameters

Listed below is the set of parameters that the DasCoin Board can propose changes upon:

License Issuing Authority
The privilege to assign a License to a Vault Account and to determine the level of license.

License Authenticating Authority
The ability to cancel the issuance of a new License to an account in the event of error.

WebEuro Issuing Authority
The privilege to transfer a WebEUR balance to a Vault Account.

WebEuro Authenticating Authority
The ability to cancel the issuance of a WebEUR balance to an account in the event of error.

Cycle Upgrade Date & Interval
The exact date of an Upgrade and the Upgrade Interval (currently set at 108 days).

Frequency
The conversion factor by which Cycles can be exchanged for DasCoins as part of the minting process.

DasCoin Distribution Rate
The number of DasCoins to be distributed at the next Interval.

DasCoin Distribution Interval
The number of Blocks until a DasCoin Distribution will Occur

Block Interval
The time it takes to create a confirmation of a single block. By default, we confirm transactions every 6 seconds. In the future, this will be decreased as we optimize the code base.
the licensing information obtained by the person or business entity.

Maintenance Period
The number of blocks that must pass before a Maintenance is performed on the Blockchain.

Maintenance Skip Slots
During a maintenance period some blocks will be skipped this parameter sets how many the system should skip while performing a Maintenance Period.

Maximum Transaction Size
This is the maximum allowable size in bytes for a single transaction.

Maximum Block Size
Maximum size in bytes that a block can be that is signed to the Blockchain.

Maximum Witness Count
This is the maximum number of Master Nodes that could be active on the network.

Audit and Integrity Verification

The DasCoin Blockchain is a cryptographically linked series of blocks. These blocks establish a permanent record of transaction that have been verified and confirmed by the Master Nodes that maintain and recording privileges of the Blockchain. Therefore, every action stored on the Blockchain has a permanent and unique identifier.

Because of these features the entire history of activities in the Blockchain can be replayed and checked for integrity at any moment. An auditor can be authorized to use programmatic tools that evaluate and check the balances of all actions that they are consistent and correct. This excludes the ability for a central actor or the operators of the Blockchain or any intrusion to be able to manipulate the contents of the Blockchain. All actions require the signature of the owner of content in order to push forward a new change. The account owners are the only ones who are capable of causing changes in their balances to occur and the operators are not capable of making malicious or forced transfer or modification of balances.

Adoption and Compensation

The system increases in utility value as more people participate in the network. To achieve the goal expanding the network, a referral-based marketing system has been built into the network's software that is designed to award each participant contribution commensurate with their individual impact on the growth of the network. Consequently, rather than use resources to cover the costs of proof-of-work mining, this network is able to incentivize its participants to expand the network.

All commissions are allocated to the participants in the form of a cryptographic asset that resides on the DasCoin Blockchain making a non-repudiable and low friction method of reimbursement which directly raises the activities of the network.

Conclusion

DasCoin has been designed to deliver attributes that will enable it to become the first cryptocurrency in the world to become adopted by the mainstream. DasCoin is structured to deliver greater security, efficiency, performance, and scalability. DasNet leverages the efficiencies of its infrastructure to incentivize its expansion. The result is a system of digital value that is built on sound money principles and positioned to be adopted throughout the world by mainstream users. As that becomes as reality, DasCoin will create prosperity at a level never seen due to its innovative structure.

DasCoin™