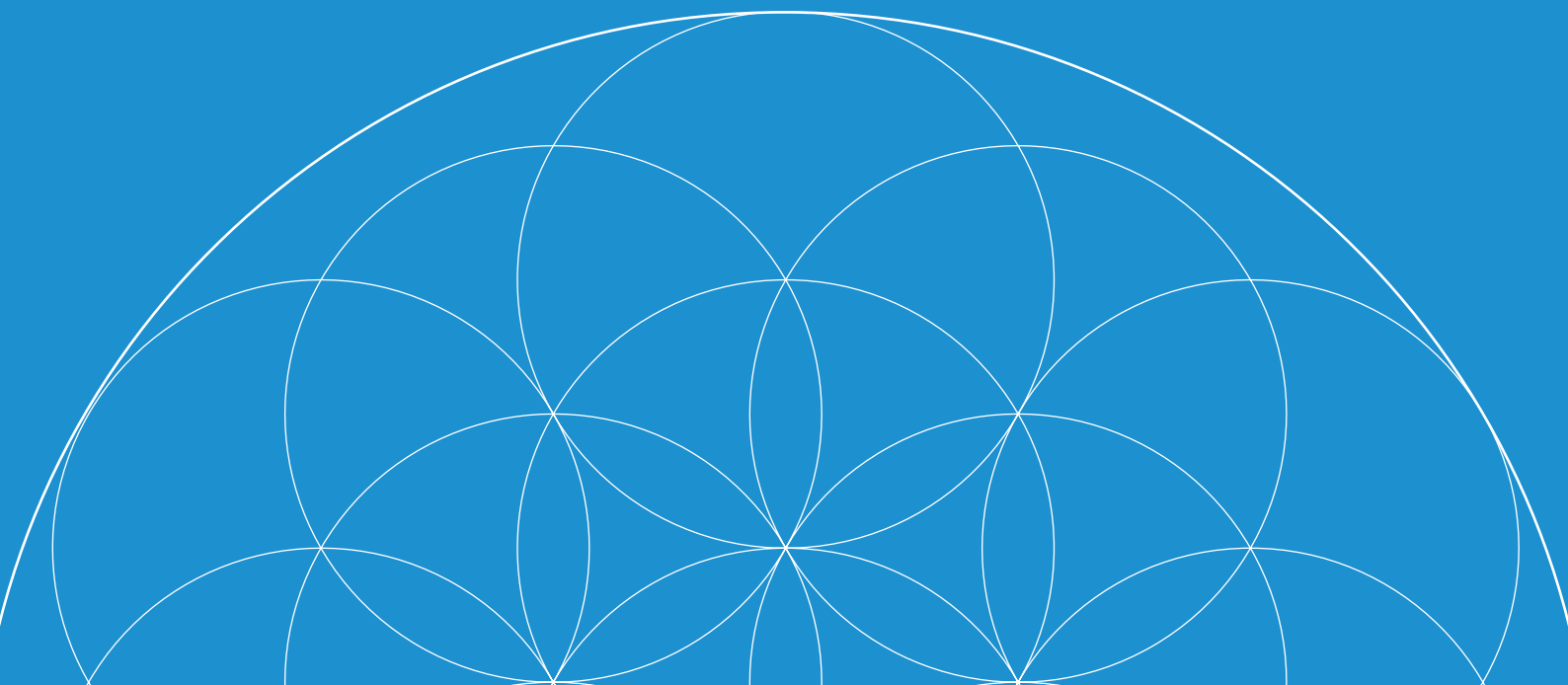
# DasCoin™

## The Currency of Trust

**Michael Mathias**

March 31st 2017



# Abstract

**DasCoin has been designed to solve the core problems inherent to storing and exchanging value.**

The DasCoin Blockchain is a mutual distributed ledger that creates and distributes cryptographic assets, and then securely facilitates their storage and exchange. The DasCoin Blockchain forms the nucleus of a digital asset system known as the DasEcosystem, which has been structured to deliver a set of value exchange solutions that offer enhanced security, greater utility, increased scalability, wider acceptance, improved efficiency, and better performance.

At the heart of the system is DasCoin, a hybrid currency designed to combine the best qualities of decentralized cryptocurrencies with the best aspects of centralized currencies – and eliminate their respective weaknesses. DasCoin is the convertible "store of value" unit that serves as the foundation of the digital asset system. The system has been designed to increase global prosperity through improvements in the quality and efficiency of the exchange of value between individuals, and businesses, financial institutions, cooperatives, and merchants.

Instead of basing value on the backing of a commodity or the declaration of a government, the value of DasCoin is based on the quality and soundness of the underlying system. Trust is fundamental to the system and has been adapted to the digital paradigm (rather than systematically eliminated). Ultimately, through a wider-distributed, more efficient, and better-calibrated system of value, prosperity can be enjoyed by a larger and more diverse global population.

# 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 is possible to digitally format a money system – experiencing significant success in the 8 years of its existence. Since its emergence, other cryptocurrencies have sprung up, but few have made real impact on the market.

The main point of impact has been the innovative technology underlying Bitcoin known as "the blockchain." The blockchain is a tool that can verify transactions with minimal third-party involvement. The names of buyers and sellers are never revealed – only their addresses within the system-and these addresses can be further obscured. Blockchain technology is part of a category known as a mutual distributed ledger. "Mutual" refers to the fact that the nodes are shared by the community, rather than owned by a central authority. "Distributed" refers to the fact that the nodes are divided among a number of locations. And "ledger" in that the system represents a sequential record of transactions.

Assembled together, the system becomes a tamper-proof, immutable record of transactions shared among a community of users and stored in multiple locations. The 2 dominant cryptocurrency models, "proof-of-work" and "proof-of-stake", have significant weaknesses. Bitcoin's proof-of-work model is a brutally inefficient system, and its decentralized structure leads to serious governance issues (as evidenced by the ongoing block-size debate). The proof-of-stake alt coins suffer from pre-distribution issues ("pre-mining" can distribute coins without transparency or justification) and an inherent lack of validity (due to the "nothing at stake" problem).

Every system of value must establish a few fundamental elements. These include defining: initial money supply, initial distribution, basis of value, expansion/contraction mechanisms of the money supply, who controls the means of production, and the allocation of inflation (and/or allocation of credit).

DasCoin offers a hybrid structure to solve the issues associated with these economics-based elements. A private, permissioned blockchain architecture has been incorporated due to its enhanced security, inherent efficiency, and ability to scale more easily (due to deployment control). Fortifying this secure foundation is the authentication of all users in accordance with banking-standard KYC (Know Your Customer) requirements and the implementation of a "hardware-required" digital wallet system. In addition, the DasCoin system integrates a powerful marketing mechanism which incentivizes growth through referral-based word of mouth promotion. The result is digital system of value that offers optimal security, world-class performance, and is poised for rapid global adoption by the mass market.

# Key Design Features

**"Proof of Value" Distribution Method**
The assurance that anyone who is distributed DasCoins directly from the DasCoin Blockchain has presented the system with a defined and recognized form of value (specifically in "Cycles", a closed-loop, single purpose currency that can only be acquired through the purchase of a system license using either Bitcoin or Euros). There are no parties (neither executives nor developers) who are able to pre-mint, pre-mine or pre-distribute DasCoins to themselves. Cycles can only be received in exchange for value transferred to the system, and Cycles must be submitted to the system in order for there to be a direct distribution of DasCoins through the minting process.

**"Proof of License" Consensus Method**
DasCoin incorporates a licensing system rather than a mining apparatus. Consensus is reached through an algorithm which randomly defines what licensed node is going to make the next block.

**Fixed Supply**
2 to the 33rd power, about 8.5 billion units (distributed over an undefined period – dependent on the internal dynamics of the system – currently projected to last 12 years).

**Fully-Authenticated Network**
Every user will be authenticated through banking-standard
KYC processes performed by a central authority.

**Convertibility**
DasCoins are minted into circulation through a conversion from Cycles. Once minted, they can be transferred directly or converted into a variety of fiat currencies and Bitcoin. Existing DasCoins will eventually be trading on a variety of exchanges and at that point it will be possible to convert fiat currencies directly into DasCoins.

**Distributed Ecosystem**
Supporting the value of the digital asset system is a global network of hardware and software systems, as well as associated products and services that are offered within this system, (including trading exchange functions and payment solutions). This network of systems interconnect many jurisdictions of the world and feature redundancies designed to assure smooth ongoing operations.

**Incentivized Marketing**
A referral-based marketing system to support the development of a global affinity group who recognize DasCoin and are interested in exchanging value through this digital asset system.

# Hybrid Features

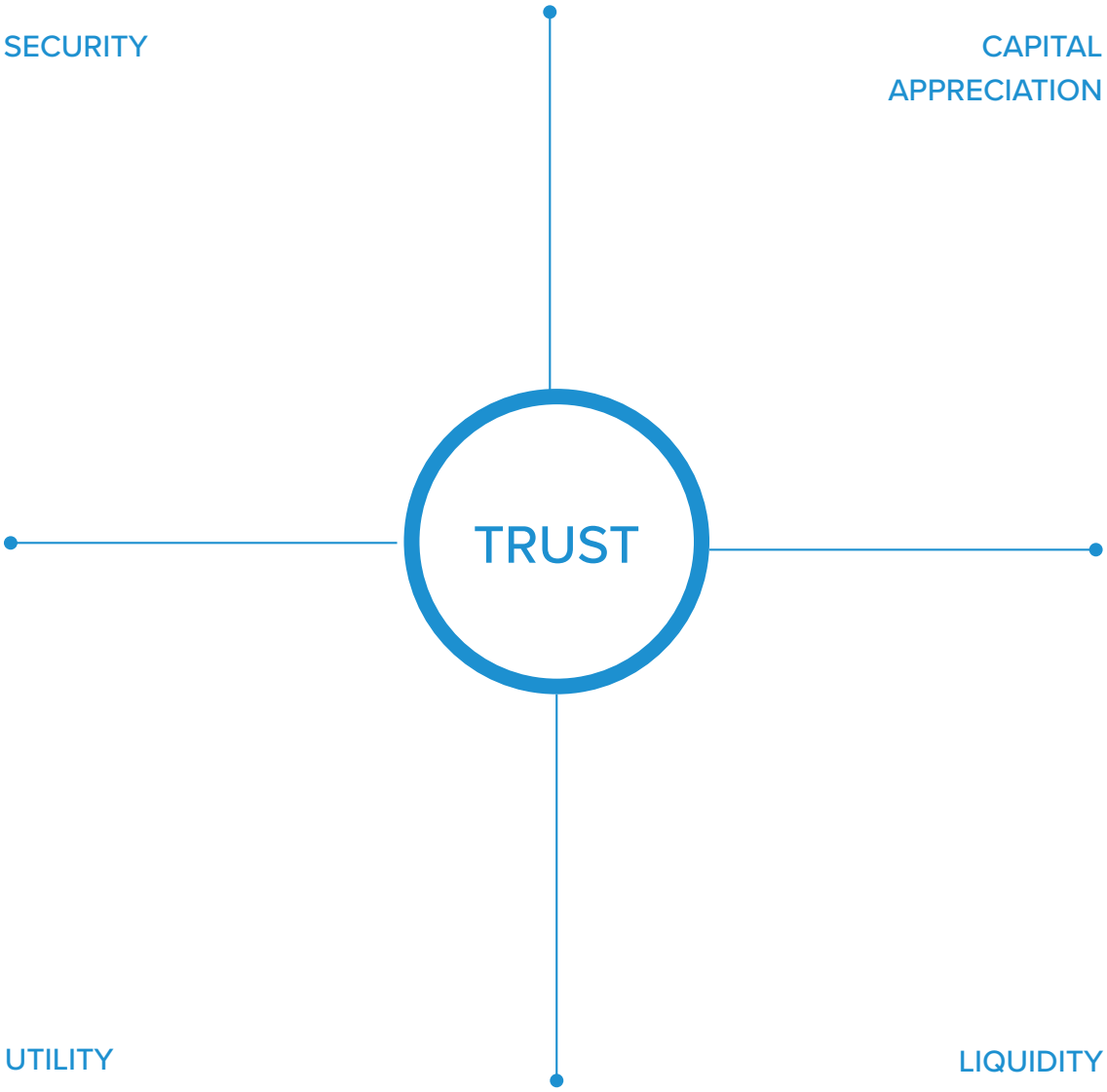
**With DasCoin, centralized and decentralized approaches have been combined to solve problems and maximize user benefits.**

- Centralized emissions of coins.
- Decentralized distribution of coins.
- Permissioned blockchain with independent verification.
- Centrally-authenticated userbase through banking-standard KYC process to support trust among participants.
- Distributed, decentralized ecosystem.
- Decentralized digital wallet system: Once issued, a coin can only be controlled through the private key of the digital wallet of the authenticated party who owns the coin. No other person, company or authority can transfer, confiscate or seize that coin.
- Privacy with transparency (and without anonymity) in the way transactions are made and recorded.
- Full compliance with regulation: Compliance with major jurisdictions and the development of industry standards.
- Instant transactions with a validation speed set at 6 seconds.
- Decentralized inflation allocation (via the minting queue and “proof of value” distribution method).

# Key Objectives

**DasCoin was created with the following objectives in mind:**

- **Security:** The entire DasCoin system must be secure.
- **Liquidity:** There must be an ability to exchange the DasCoin unit for other forms of value.
- **Utility:** There must be multiple ways to use DasCoin within the marketplace.
- **Capital Appreciation:** The unit must function as a true store of value. As the value within the ecosystem grows, the value of the DasCoin unit must also grow.



# Guiding Principles

**Trust:** A prime objective of DasCoin is to use the infrastructure of a digital asset system 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 and maximize the efficiency and utility of the network.

2. Programmatically ensuring 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.

4. Ensuring that the accuracy and level of operations of the permissioned blockchain are verified by a qualified third-party accounting firm.

5. Providing a high degree of transparency while also ensuring that the privacy of all participants of the system is well preserved.

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

**Privacy:** The system was designed to preserve the privacy of individuals without the need for anonymity. Transparency is maintained provided there is no compromise to either system security or the preservation of the privacy of network participants.

**Convenience:** Wherever possible, the system incorporates features that improve convenience and ease of use. Security and convenience are often diametrically opposed, but the system has been designed to optimize the balance of these 2 important characteristics.

**Simplicity:** An overarching goal was to keep the system as simple as possible, particularly related to all user interactions.

# Definitions

**Private Key**
A secret code that provides access to and control of cryptographic assets. The system's private key format is a 32-byte number generated through a sufficiently random method of generation.

**Public Key**
A code that can be shared but is paired with the Private Key. The system's public key format is 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, and exchange functionalities.

**DasNet**
The high-speed node network on which DasCoin and the entire DasEcosystem exists.

**DasCoin Blockchain**
A private, permissioned blockchain architecture that features enhanced security, inherent efficiency and improved scalability.

**Vault Account**
An account within the digital wallet system held by a person or business entity who has been authenticated. This account holds the licensing information for that particular 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 in exchange for DasCoins.

**DasCoin**
A convertible "store of value" unit at the center of the digital asset system. DasCoins are produced and distributed in exchange for Cycles that have been 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. A queue is formed upon Cycles being submitted to the system. A certain number of DasCoins are then created every 10 minutes and distributed based on the relevant Frequency and parameters within the queue.

# Definitions

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

**DasCoin Minting Block**
The amount of DasCoins distributed at the end of each Minting Interval.

**DasCoin Minting Interval**
The 10-minute duration between DasCoin Minting Blocks.

**DasCoin Minting Rate**
The number of DasCoins that will be distributed during the elapsing of a DasCoin Minting 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. Only once all required fields are filled and each operation is signed by the respective keys 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 sequential application of blocks means that there cannot be any inconsistencies between 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 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.

### Minting Blocks

A Minting Block is the direct distribution of newly minted DasCoins that occurs at the end of each Minting Block Interval (currently set at 10 minutes). Each Minting Block is made by a Master Node and cryptographically linked to the previous Minting Block. The resulting DasCoins are directly transferred to WebWallet Vaults in accordance with the Minting Queue.

# Transaction Ledger

**Deep Vault Contract**

A Deep Vault Contract is a smart contract that exists on the DasCoin Blockchain. It requires the owner of a WebWallet Vault to transfer a certain number of DasCoins to deep storage for an agreed upon period of time (the term of the contract). In deep storage, the DasCoins are not able to be transferred until the term has expired, and will be automatically transferred back to the original vault unless the contract holder agrees to rollover the balance for another term.

As an incentive for agreeing to store a certain amount of DasCoins, the owner of the DasCoins is provided a share of a Reward Pool. Reward proceeds are distributed directly from the DasCoin Blockchain into the deep vault of the contract holder. Each initial Deep Vault Contract is worth one share of the Reward Pool, and the reward is shared among all the current contract holders during that period.

There are 3 different types of Deep Vault Contracts. Each requires a different Qualifying Transfer, a different Commitment Term, and each provides a different Reward Pool. Each also entitles the contract holder to a certain amount of voting influence in the system.

**Voting Contract**

This contract requires 10,000 DasCoins to be committed for a period of 2 years. The Reward Pool for this contract is an additional 10% of all the DasCoin minted each week, and is distributed on a weekly basis. There is no limit to the number of Voting Contracts a person or entity can hold.

**Ledger Contract**

This contract requires 100,000 DasCoins to be committed for a period of 3 years. The contract holder must also run 10 Ledger Nodes to be qualified to participate in the Ledger Reward Pool. The system will verify that these nodes have been active throughout the period prior to distributing the contract holder's share of the reward. The Reward Pool for this contract is an additional 6% of all the DasCoin minted in a 2 week period, and is distributed every 2 weeks. There is no limit to the number of Ledger Contracts a person or entity can hold.

# Transaction Ledger

**Master Contract**

This contract requires 1,000,000 DasCoin to be committed for a period of 5 years. The contract holder must also run a Master Node to be qualified to participate in the Master Reward Pool. The system will verify that this node has been active throughout the period prior to distributing the contract holder's share of the reward. The Reward Pool for this contract Is an additional 3% of all DasCoin minted in a 3 week period, and is distributed every 3 weeks. There is a limit of 3 Master Contracts per person, entity or related parties.

| Contract | Qualifying Transfer | Commitment Term | Reward Pool | Votes |
|---|---|---|---|---|
| Voting Contract | 10,000 DasCoins | 2 years | 10% | 1 |
| Ledger Contract | 100,000 DasCoins | 3 years | 6% | 20 |
| Master Contract | 1,000,000 DasCoins | 5 years | 3% | 300 |

**Rollover**

An extra incentive is provided to each contract holder for agreeing to commit to an additional term prior to the expiration of the current term. By "rolling over" their contract, the contract holder will get 2 shares of the Reward Pool, rather than just 1 as would normally be the case. Each subsequent commitment will be accompanied by an additional share of the pool, so upon agreeing to a second rollover the contract holder would receive 3 shares, rather than the normal single share, during that upcoming term. Each Rollover agreement adds another Reward Pool share throughout the terms of the upcoming contract.

# Transaction Ledger

**Super Blocks**
A Super Block is a large distribution transaction that updates the state of the Blockchain Ledger on a specific interval. Each Super Block is made by a Master Node in accordance with a series of smart contracts, and each Super Block is integrated into the DasCoin Blockchain through a cryptographic link to the previous standard block. The production of Super Blocks does not delay or interfere with the production of Minting Blocks and therefore does not impact the Minting Queue.

**Voting Blocks**
10% of the Minting Block production for a 1-week period. Distributed directly to deep vault accounts.

**Ledger Blocks**
6% of the Minting Block production for a 2-week period. Distributed directly to deep vault accounts.

**Master Blocks**
3% of the Minting Block production for a 3-week period. Distributed directly to deep vault accounts.

**Treasury Blocks**
1% of the Minting Block production for a 4-week period. Distributed directly to a Treasury account controlled by the DasCoin Board. The proceeds from these blocks are designed to pay for the administration of the system (Executive Director, staff and Board Directors) as well as fund awareness marketing campaigns.

The production of Super Blocks is simply a reallocation of the ultimate distribution of the total number of DasCoins. Rather than distribute the final amount of DasCoins solely through the production of Minting Blocks, the system will incentivize holders of DasCoins to store (or save) a portion of their holdings. This dynamic benefits the overall stability of the system. The system also benefits from the Community nodes that are created by the Super Blocks. This creates greater decentralization, and enhances the overall stability of the DasNet infrastructure.

# 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 are therefore useful for both increasing the footprint of the DasCoin Consensus Network and permitting connectivity to reach farther without requiring the need to assign authority to node. Transaction propagation is accelerated because of Ledger Nodes.

**Voting Nodes**

Voting Nodes are non-authoritative influencers of the DasCoin Blockchain. These nodes do not control any of the daily functions of the DasCoin system, but fully control who sits on the DasCoin Board and what proposals are passed within the system. Voting Nodes represent significant stakeholders who have demonstrated (through their commitment to hold at least 10,000 DasCoins for a period of 2–5 years) that they have a long-term view on DasCoin, and therefore are given the privilege of influence over chain governance. Each Voting Node may sign a transaction with their corresponding private key and thus express an opinion on issues regarding chain governance.

Voting takes place within a dedicated section of the WebWallet and requires authentication by a dedicated 2-factor hardware device (i.e. The Validator). Votes can occur individually or in multi-vote blocks, such as when a specific wallet account has several Deep Vault Contracts or one or more higher-level Deep Vault Contracts. Any qualified Voting Node can initiate a proposal. The DasCoin Board is responsible for organizing and presenting the proposals to the Voting Node population. There is also a mechanism within the voting system that allows the Voting Nodes to directly present a referendum to their membership without going through the Board review process (to prevent the Board from withholding a certain proposal from the Voting Nodes).

Each account holder may commit to as many Voting Contracts as they desire and receive that many number of votes in the system. Each vote is of equal weight in chain elections and referendums. The purpose of Voting Contracts is to enforce users to have a locked balance of DasCoin as stake in the system and thus have a vested interest in preserving their commitment.

# Decentralized Consensus

The length of the contract (2 years) is set with the expectation that the votes will be rationally biased toward longer term growth of value over short term gains – as commitments are locked and cannot be withdrawn to profit from short-term market dynamics.

**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. This protocol is followed for the production of all types of blocks within the blockchain.

**Software Updates**

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. This allows the DasCoin stakeholders to incorporate feature requests and for developers to optimize the performance of the software.

Due to the system's hybrid structure, there is the capacity for centralized deployment once a software update has been approved by at least 51% of the Master Nodes. Centralized deployment eliminates the possibility of there ever being what is known as a "hard fork," in which the currency system splits into 2 separate networks. This outcome is the product of internal disagreement among the production nodes of the system, and causes many negative outcomes. A hard fork is a statistical inevitability for all decentralized crypotocurrencies due to their operational structure. On the other hand, a hard fork is impossible within the DasCoin system. Upon the approval of a software update, all Core Nodes are updated and all Community Nodes in agreement are also updated. This group will account for at least 51% of the Master Nodes and will continue to operate the DasCoin Blockchain. Any remaining Community Nodes that refuse the software update will no longer be recognized within the operation of the DasCoin Blockchain and will no longer receive their Super Block Distributions.

**Privacy**

The Dascoin Blockchain is a permissioned system, meaning that all user accounts must be verified and approved by a registrar authority (which in the case of user accounts is handled through the digital wallet system).

We define the "state" as the consensus about user data (accounts, balances etc.) Unlike Bitcoin derivatives, user state exists on all nodes as in memory data and it can be freely accessed.

# Decentralized Consensus

The state is maintained through network consensus by following the longest available chain of blocks. Nodes can replay that longest path by applying each recorded transaction in order and reach the current state (or the state at the time of any block in the past).

Because state is regularly accessed and modified by the node application it cannot be stored in an encrypted format on disk (as a matter of fact the data must reside in RAM for performance reasons, making access control more difficult).

The assumption within the DasCoin Blockchain is that all data on the blockchain is public. User accounts (and thus the balances that are linked to account IDs) do not store personally-identifiable information. All private data is stored on separate, private authentication servers in encrypted cold storage. Consequently, only the users themselves know the ID of their account and thus keep their privacy from outside observers.

In order to achieve transparency of operation, the DasCoin Blockchain must be opened to the public. This requires that the block explorer (i.e., DasCoinExplorer.com) show unfiltered blocks with all the data from transactions. Through participation in Deep Vault Contracts, users are able to deploy their own Ledger Nodes to observe the Blockchain and query the state (balances, accounts and other data).

The authentication server can reveal user data for KYC validation purposes to comply with legal regulation. The users can be made aware of that fact (and the necessity to comply with the law).

Within this privacy model, trust must be placed in the authentication service of the DasCoin network. The user still has a reasonable expectation of privacy in the system as their balances are not known to external parties. KYC information is also provided in the current cryptocurrency exchange systems by legal requirement. The authentication service has a strong incentive not to divulge the private information to outside parties as it would harm the value of the network. It also reduces the amount of trust the user must place in the network. Since all transactions are public, there is no possibility for manipulation of balances and user state.

The only requirement is that the authentication servers are kept secure from intrusions. This however is a much easier task then securing the whole network as the attack surface is much smaller, so access control can be tightly regulated. If data is properly secured and shared, a potential intrusion does not necessitate a total loss of privacy as the attacker only gains a certain amount of private data.

# High Speed Node Network

The DasEcosystem exposes new power and possibility as a Blockchain and Cryptocurrency since Master Nodes only need to store their private signing key and be authenticated with the rest of the network. This means that the Master Nodes only need 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 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 specifically designed state-of-the-art network architecturre that serves a reliable network and allows global scaling.

**Hardware Infrastructure**

Master Nodes are exclusively hosted in data centers based on a requirement 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 2 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.

DasNet will have a total of 33 Core Master Nodes operating in data centers in 33 different jurisdictions throughout the world. Core Master Node installations will occur at a pace of approximately 2 per month. There will also be approximately 3,000 Core Ledger Nodes running on DasNet. In addition, Deep Vault Contracts will lead to thousands of Community Master and Ledger Nodes being added to the DasNet infrastructure.

**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.

# Middleware

**Core Development Team**

The hardware infrastructure is implemented and maintained by the Core Development Team. All software infrastructure is developed and maintained by the Core Development Team. The Board is responsible for ensuring that the Core Development Team acts in the best interest of the entire ecosystem. Master Nodes are under the control of ecosystem executives, Board Directors, and significant stakeholders from the DasCoin community. No individual or company is permitted to control more than 3 Master Nodes within the DasNet infrastructure.

# Licensing System On-Boarding

In order for a person or entity to become an active participant in this authenticated network, they must obtain a License. The Blockchain software allows for a service to be authorized to connect and register new accounts. The Value (in the form of Euros or Bitcoin) that 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 to take full advantage of the opportunities created by the License.

**Vault Accounts**

Vault Accounts hold personal information of the user and these are the accounts that are actually receiving the 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. Vault Accounts have transfer restrictions depending on license level and authentication level. For a Vault Account to be in use, it must be connected to 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 trading 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. A Wallet Account holder can also access a variety of functions through the Wallet, including voting and the operation of Community Ledger Nodes or Community Master Nodes (corresponding to Deep Vault Contracts).

**Tethering**

All Vault Accounts must be connected to a Wallet Account. The 2 types of accounts become tethered and are then inextricably linked. 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 to perform a successful tethering transaction. This process is initiated by a secure invitation that is sent through a combination of email and SMS text message by the licensing entity.

**KYC & AML (Know You Customer & Anti-Money Laundering)**

Each Vault Account must be licensed for a person or entity to access DasNet. The license level and corresponding KYC levels also determine the daily amounts a Vault Account is eligible to transfer to the Wallet Account. A higher license level enables the person or entity to increase their level of authentication 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 account holders to be identified and in good standing before engaging in commerce with other participants of the DasEcosystem. This type of authentication protocol results in a higher level of integrity amongst participants and is likely to lead to more acceptance within regulated jurisdictions throughout the world.

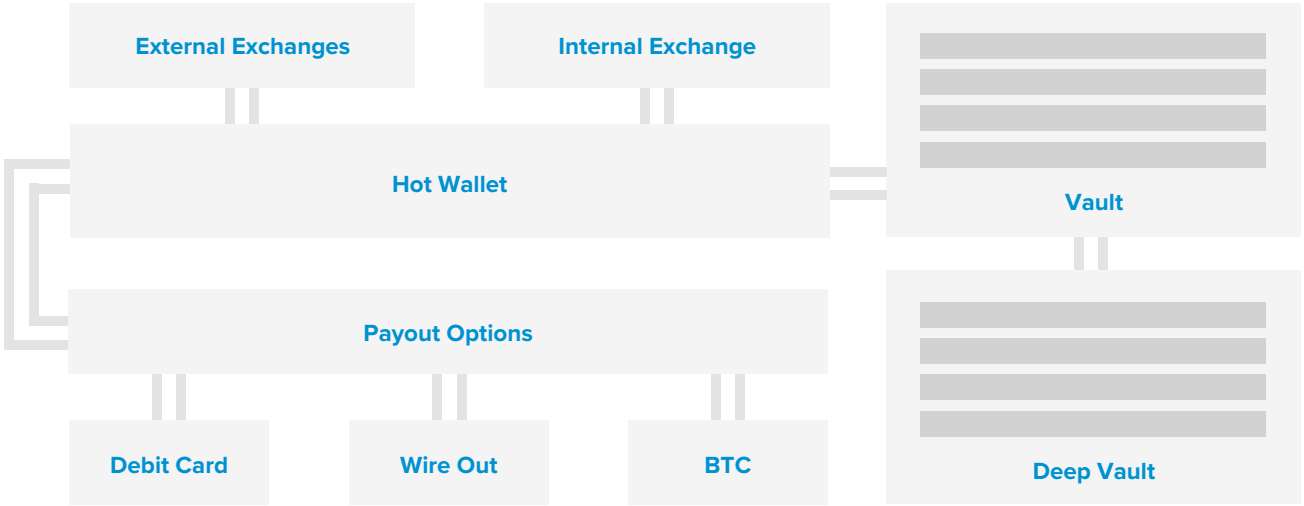
# WebWallet

WebWallet is a secure access point for users to access relevant data on the DasCoin Blockchain, and interact with the global state by way of signing transactions. It is a cryptographic web-based wallet with the client front end running on the user's browser and the application server backend hosted on an internet web server. The WebWallet serves as the user's point of entry into the secure Dascoin Network. Each WebWallet account links the users to their vaults and wallets and is used to store and validate personal KYC and AML information. Users authenticated through WebWallet can access their relevant data from the global blockchain state – balances from vaults, license purchases, history of transactions etc.

WebWallet relies on a cryptographic hardware store for managing keys and securely signing blockchain transactions. This proprietary hardware device is known as The Validator and has the ability to generate and store ECDSA private keys corresponding to the users blockchain vaults. The Validator is also secured with a PIN/passphrase that prevents missuse and theft of keys.

When signing blockchain transactions, WebWallet interfaces with The Validator hardware device. The user must first unlock their Validator before the required private ECDSA key can be transferred into the browser memory of the javascript client application upon confirmation of a transaction. No DasCoin transaction can be made without validation through this cryptographic hardware device. This system provides the highest level of safety and security in the authentication of transactions. The key is stored in the memory for the shortest possible time required to sign the transaction upon which it is purged from the client memory. The private key is never 'hot' – it never crosses the wire, not even in encrypted form.

The user can back up a mnemonic consisting of 24 words used as entropy for generating the private key. In case of theft or loss of the hardware device, the user can use the mnemonic to reconstruct the original private key, restoring access to their account.



# 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 Cycles to the network and then be assigned a place in the DasCoin Minting Queue. On a first-in-first-out basis, DasCoins are distributed to the account that is next in line of the distribution queue. At each DasCoin Distribution Interval a specific amount of DasCoins are distributed to participants in the queue.

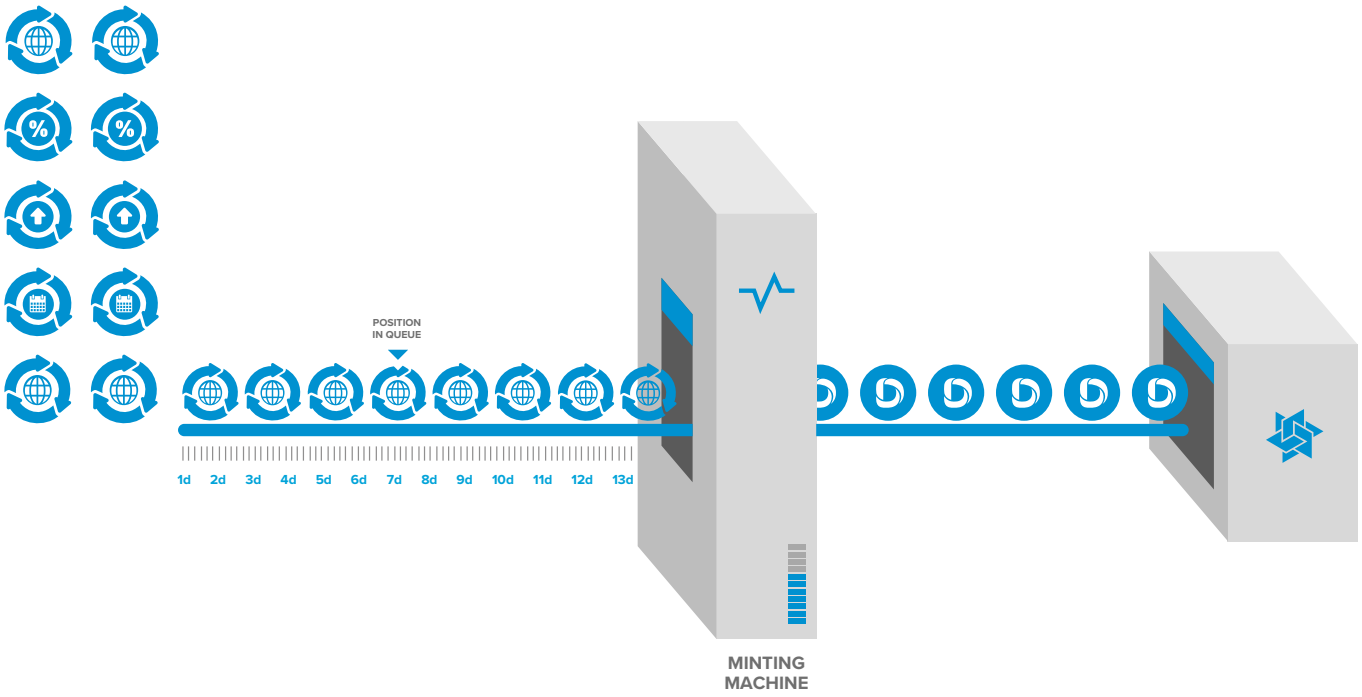
The amount of DasCoins to be received is regulated by an adjustable conversion factor called Frequency in such a way that the amount of Cycles submitted divided by the Frequency equals the number of DasCoins that will be distributed to that person. The account is deducted Cycles at the time of submission 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
```

# DasCoin Minting

Periodically, in accordance with a predetermined Upgrade Interval, all Cycle balances will experience an Upgrade and those balances in the accounts will double. If Cycles are already in the DasCoin Minting Queue, these Cycles will be unaffected (unless they are associated with an account that has a Frequency Lock).



# Blockchained Internal Exchange

The DasCoin Blockchain also incorporates a decentralized exchange that trades, settles, and clears over the Blockchain autonomously. This way, licensed users 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 can withdraw Euros directly to their bank account from their WebWallet account.

# Governance of the Network

**Voting Nodes**

DasCoin governance begins with Voting Nodes that are operated within wallet accounts that hold at least 10,000 DasCoins and have committed to holding these DasCoins for at least 2 years through a Deep Vault Contract. All Voting Nodes 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.

**The DasCoin Board**

The DasCoin Blockchain enables a governing board to regulate the parameters of the network. The DasCoin Board will be comprised of members elected by the Voting Nodes. 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 terminate their access to the network.

The Board itself has no control on the state of the database or the construction of the DasCoin Blockchain and is programmatically prevented from making any changes to it. Since 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.

The Board is designed to consist of 7 individual Directors, each of whom is bestowed with full voting privileges. Generally, each Director serves for a 6-year term, though initial Directors will be serving staggered terms (of 2-6 years) to ensure continuity of experience. A minimum of 3 Directors are required for the governance of the DasCoin ecosystem, and as many as 9 may serve on the Board.

In addition, there is an Ombudsman member of the Board, who does not vote and does not hold any responsibilities within the Board, but who attends all Board meetings and provides a degree of independence and transparency to the Board's governance process.

Finally, there is an Executive Director who works for the Board and is responsible for ensuring that all of its decisions and initiatives are enacted and enforced. The Executive Director attends all Board meetings but is not permitted to vote. The Executive Director is responsible for directly overseeing all Chain Authorities.

# 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 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.

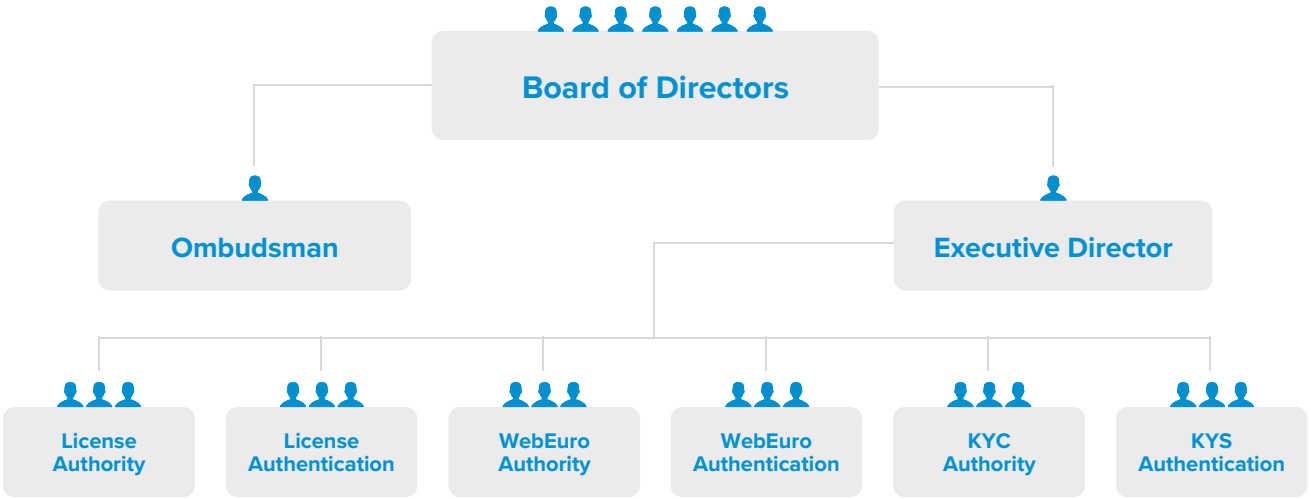
Each authority role is set up in such a way that:

**1.** There is no way for the authority to make a meaningful unwanted impact on the state of the network as the network can fall back to a failsafe state.

**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 being marked as untrustworthy, shut off from the network and penalized.



# Governance of the Network

**Operations**

The Board sets the procedures and ensures the proper execution of the following: the level of the Frequency at each 2-week interval; the size of the Minting Blocks at the start of each Upgrade Interval; the size of the Super Blocks and Treasury Blocks; the proposals to be submitted to the Voting Nodes, the use of funds from Treasury Blocks; the authorization of Master Nodes and Ledger Nodes within the DasNet infrastructure; intervention at times of crisis, and other elements (listed below under Board Parameters).

The Executive Director oversees the performance of all chain authorities and KYC functions, manages the flow of proposals for the Board to consider, facilitates referendums if the proper thresholds have been surpassed, is responsible for enforcing all Board initiatives and decisions, and is fully accountable to the Board for all operations within the system.

Chain authorities oversee the issuance and authentication of Licenses and WebEuros, under the supervision of the Executive Director.

Frequency is adjusted every 2 weeks. The process involves the Board selecting which of a range of algorithms best reflects the current growth state of the network. The primary factors considered include: overall amount of Cycles in the system; amount of Cycles authorized in the most recent 2-week period; velocity of Cycle growth in previous periods, and projected Cycle growth within the system.

Upgrades automatically occur on a system-wide basis on specific dates, starting 108 days from the launch of the DasCoin Blockchain. It is unlikely that this interval will be altered at any point in the future, but it remains within the capability of the Board to make such an adjustment should they feel it is needed. All Deep Vault Contracts also function automatically. Essentially, the minting process, Upgrades and Deep Vault Contracts are all smart contracts that are automatically executed and built directly into the DasCoin ecosystem.

**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.

# Governance of the Network

**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. The Upgrade Interval is current set at 108 days and is not expected to ever be changed.

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

**Block**
A measurement for accumulated transactions. The system currently records a block in accordance with a designated period, known as a Block Interval.

**Block Interval**
The time it takes to create a confirmation, of a single block of transactions.
By default, transactions are confirmed every 6 seconds. In the future, this will be decreased as the code base is further optimized.

**Minting Block**
The amount of DasCoins distributed at the completion of each Minting Interval.

**Minting Interval**
The time it takes for a Minting Block to be created. The default Minting Interval of the system is 10 minutes, and is not expected to ever be changed.

**Maintenance Period**
The number of blocks that must pass before 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.

**Super Block**
The amount of DasCoins distributed at the completion of each type of Super Block Interval. The size of Super Blocks are expressed as a percentage of the cumulative DasCoins distributed by Minting Blocks within that Super Block Interval. There are 3 types of Super Blocks, and each corresponds to a particular Deep Vault Contract: Voting Super Blocks, Ledger Super Blocks, Master Super Blocks.

# Governance of the Network

**Super Block Intervals**
The time it takes for Super Blocks to be created. There are 3 Super Block Intervals within the system, each of which corresponds with a type of Super Block. The Voting Super Block Intervals are 1 week in duration, the Ledger Super Block Intervals are 2 weeks in duration, and the Master Super Block Intervals are 3 weeks in duration.

**Treasury Block**
The amount of DasCoins distributed at the completion of a Treasury Block Interval. Like Super Blocks, Treasury Blocks are expressed as a percentage of the cumulative DasCoins distributed by Minting Blocks within the Treasury Block Interval.

**Treasury Block Interval**
The time it takes for a Treasury Block to be created. Treasury Block Intervals are 4 weeks in duration.

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

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

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

| | |
|---|---|
| Account hash/name length: | between 3 and 63 characters |
| Transaction size: | 1024B |
| Time between blocks: | 6 seconds. |
| Time between maintenance intervals:w | 1 day |
| Maintenance duration (# of blocks skipped): | 3 blocks |
| Time between Upgrades: | 108 days |
| Time between minting (Minting Interval): | 10 minutes |

# Overall System Efficiency

Bitcoin and chains based on Bitcoin forks rely on a database of UTXO objects to track token balances for each address/account. In Bitcoin, every transaction consumes (spends) outputs from prior transactions and produces new outputs to be consumed by future transactions, forming a new Unspent Transaction Output (UTXO) that can only be consumed once. Although this model has certain beneficial mathematical properties and it is used to prevent double spend in bitcoin, it also suffers from severe limitations: it is unnecessarily complicated, and is inherently stateless and thus not naturally suited to applications that are inherently stateful, such as manipulation of custom assets and saving state of smart contract execution.

The DasCoin Blockchain relies instead on a shared chain state - an in memory database of stateful objects related to user data such as account, balances of DasCoin (and possibly other assets), minting information such as the DasCoin Minting Queue, information regarding the execution of smart contracts, etc. The Blockchain nodes form the state by applying transactions from the previous blocks. The state consensus is reached by following the longest chain of blocks the node can see. Blockchain state is fully reproducible by applying the transactions in order.

One of the main goals of the DasCoin Blockchain are fast transactions. Because each node stores the shared state in memory, transactions can quickly be validated across the network. This greatly increases the number of transactions that can be included in a block, increasing the overall throughput of the network. Because there is no demanding Proof of Work required to sign a block, each witness can quickly collect and verify transactions against the global state, form a block of valid transactions, sign them with their block signing key and transmit the signed block to the rest of the network. Nodes can also quickly roll back transactions in case of consensus failure, both in case the block being rejected (due to being on a shorter fork during fork resolution) or due to the transaction expiring without being included in any blocks.

# Blockchain 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 record 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 that the balances of all actions 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.

As part of responsible Board oversight protocol, it is required that an independent third-party accounting firm be hired to verify the authenticity of all Blockchain activities. This firm will be paid through Treasury funds under the control of the Board and will have access to at least 2 Ledger Nodes, for which they will be given full access to query and test in accordance with the verification protocol they have designed. The verification of the accuracy and integrity of the DasCoin Blockchain will occur on a monthly basis and the outcome of these testing protocols will be made available to all participants within the DasNet system.

The purpose of the monthly Blockchain integrity verification protocol is to increase the trust within the system. The protocol has been designed to protect the security of the network and the privacy of its participants while still providing a third-party accounting firm with full access to active Ledger Nodes within the system and complete transparency regarding overall operations of the DasCoin Blockchain.

# Expansion and Adoption

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's 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, the network offers incentives to its participants to expand the network.

This type of incentive system is made possible through the inherent efficiencies of the Proof of License consensus model. Rather than incur the financial burden of protecting an openly-configured network of peer-to-peer servers, the DasCoin Blockchain employs a significantly more efficient method of reaching consensus.

By balancing aspects of centralization with elements of decentralization, the system is capable of managing itself through a sufficiently randomized but highly efficient consensus method. By incorporating closed-system architecture, the network is able to benefit from all the advantages of blockchain protocol but without all the expense, inefficiencies and security considerations associated with decentralized open-system architecture. The resulting efficiencies of this permissioned blockchain model when combined with a licensing arrangement enables the network to provide incentives for advocates to promote and expand the benefits of the network throughout the world.

The system is designed to account for the risks inherent to a new network and to reward participants commensurate with their impact on the growth of the network. This dynamic provides powerful marketing trust to the expansion of the network.

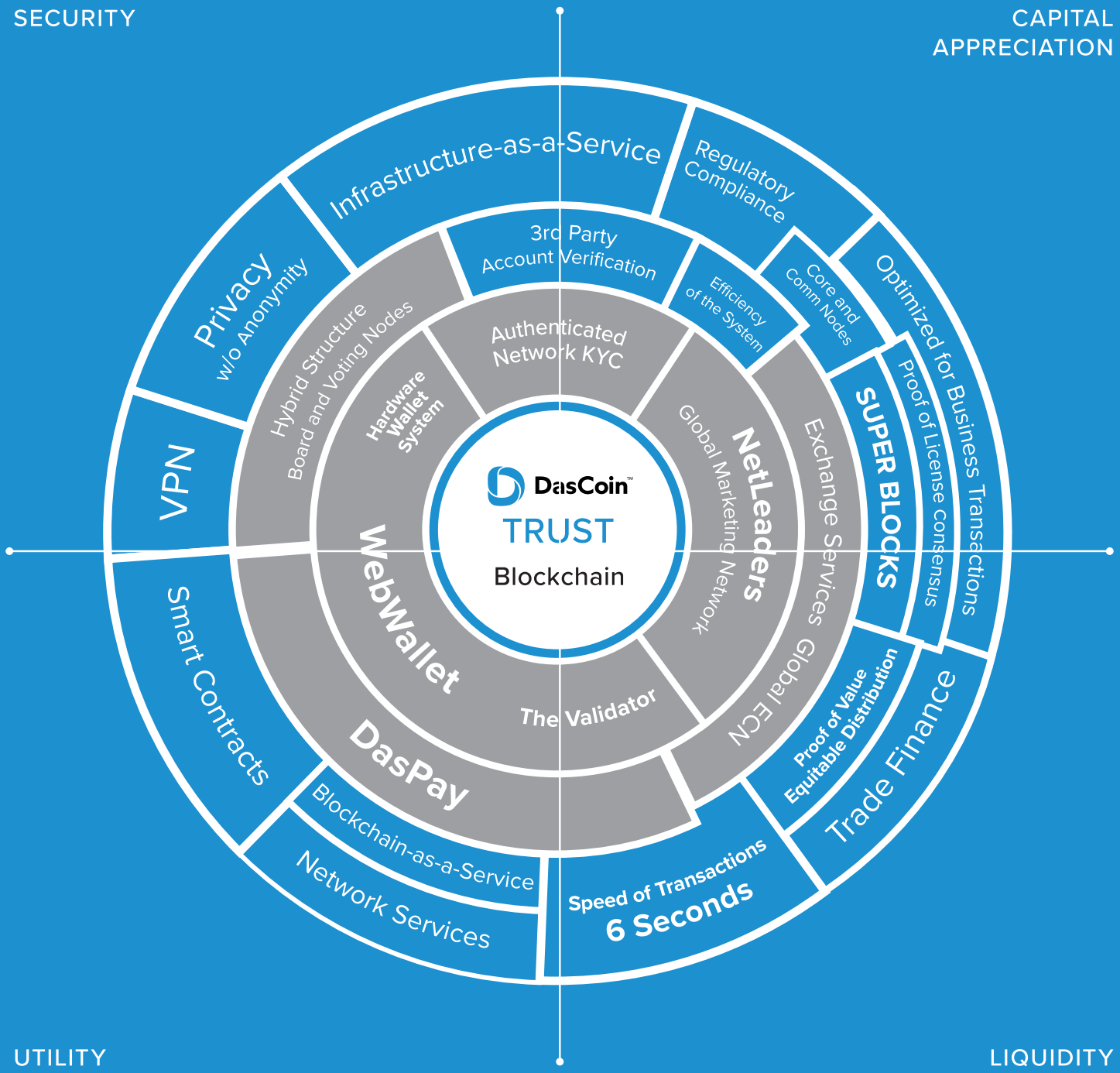
# Conclusion

Until now, there has not been enough emphasis on the infrastructure requirements at the foundation of blockchain deployments, specifically the elements that relate to reliability, availability, scalability and maintainability. These are crucial factors in ensuring that the blockchain can play a viable role in the financial lives of mainstream users. An entire level of quality assurance has been from blockchain technology mainly due to the inherent limitations of the decentralized nature of most blockchain technology.

DasCoin has been designed to address the issues that have prevented digital currency from being adopted by mainstream users. DasCoin is structured to deliver greater security, efficiency, performance, and scalability. The DasCoin ecosystem also 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 ideally suited to attract mainstream users throughout the world.

The outcome of the DasCoin system is the full realization of the Internet of Trust, in which authenticated users can trade all kinds of assets over a specialized virtual private network. What becomes possible is a world filled with borderless transactions conducted in all kinds of different digital assets and completed anywhere in the world, at any time of day or night, instantaneously, securely and for virtually no cost. And this is just the beginning of what's possible with the DasCoin ecosystem.

It's by adapting trust to the digital paradigm that we can access all of these possibilities. Trust is the currency of DasCoin, and DasCoin is the currency of trust. As the reality of this comes to light, DasCoin will unlock unprecedented levels of prosperity throughout the world.


SECURITY
CAPITAL APPRECIATION
UTILITY
LIQUIDITY
Infrastructure-as-a-Service
Regulatory Compliance
Optimized for Business Transactions
Proof of License Consensus
SUPER BLOCKS
Core and Comm Nodes
Efficiency of the System
3rd Party Account Verification
Authenticated Network KYC
Hybrid Structure Board and Voting Nodes
Privacy w/o Anonymity
VPN
Smart Contracts
Blockchain-as-a-Service
Network Services
Hardware Wallet System
WebWallet
DasPay
DasCoin™
TRUST
Blockchain
NetLeaders
Global Marketing Network
Exchange Services
Global ECN
The Validator
Proof of Value Equitable Distribution
Trade Finance
Speed of Transactions
6 Seconds