Abstract

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

The Das Blockchain is a mutual distributed ledger that creates and distributes cryptographic assets, and then securely facilitates their storage and exchange. The Das 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 10 years of its existence.

The main point of impact within this emerging realm 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 two 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. 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
A unique method was used for initial creation and distribution of DasCoin units. No parties (including executives and developers) were able to pre-mint, pre-mine or pre-distribute units of DasCoin. Only parties who presented the system with verified value were issued units of DasCoin in a process known as “minting”.

“Proof of License” Consensus Method
The Das Blockchain incorporates a licensing system rather than a stake-based system or mining apparatus. We had referred to it as “Proof of License” in the original White Paper, but it has come to be known as “Proof of Authority.” Consensus is reached through an algorithm which randomly defines which licensed node is going to make the next block.

Fixed Supply
The total supply of DasCoin is 3,294,166,501 units. All of these units are in circulation. There will never be any more units of DasCoin created.

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

Convertibility
Units of DasCoin can be transferred directly or converted. DasCoin currently trades on a number of public cryptocurrency exchanges.

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.
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: The system has been designed so that a coin can only be controlled through the private key of the digital wallet of the authenticated party who owns the coin – this protocol ensures that 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.
- Compliance with applicable regulations in major jurisdictions.
- Near-instant transactions with a validation speed set at 3 seconds.
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. The system should function in the following manner: as the value of the ecosystem grows, the price of the store of value unit increases.
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 stakeholders 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 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.

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.
Definition

**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.

**DasCoin**
A convertible “store of value” unit at the center of the digital asset system.
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.
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 Das 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.

**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 based on authorization eliminates the possibility of there ever being a traditional “hard fork,” in which the currency system splits into two 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 cryptocurrencies due to their operational structure.
Decentralized Consensus

On the other hand, it is impossible for the DasCoin system to split into two separate systems, though only one of the resulting two systems will be supported by the Das node network. Upon the approval of a software update, Master Nodes are updated accordingly.

Privacy

The Das 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 DasWallet system or through external exchange systems).

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.

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 Das 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 Das 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.

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.
Decentralized Consensus

The only requirement is that the authentication servers are kept secure from intrusions. This however is a much easier task than 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 architecture that serves a reliable network and allows global scaling.

**Hardware Infrastructure**

Master Nodes are designed to be hosted in data centers based on a requirement that access to the server rack is physically secured. They can be 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, powerful servers provide the efficiency to scale to very high traffic levels of global utilization.

DasNet has been designed to have a system of 33 Core Master Nodes operating in 33 different jurisdictions throughout the world.

**Software Infrastructure**

Connectivity to the Das 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 Das 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 immutable cryptographic connection between all activities defends the principles of the Das Blockchain.
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 companies via the direction and instructions provided by the senior-level executives of those companies. No company is permitted to control more than 3 Master Nodes within the DasNet infrastructure.
DasWallet is a secure access point for users to access relevant data on the Das 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 DasWallet serves as the user’s point of entry into the secure Dascoin Network. Each DasWallet account links the users to their vaults and wallets and is used to store and validate personal KYC and AML information. Users authenticated through DasWallet can access their relevant data from the global blockchain state – balances from vaults, history of transactions etc.

DasWallet 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 misuse and theft of keys.

When signing blockchain transactions, DasWallet 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.
System On-Boarding

DasWallet Accounts
DasWallet is one access point for handling digital assets from the Das Blockchain. Users acquire an account via the DasWallet.com website. DasWallet accounts hold personal information of the user. All DasWallet accounts are registered on the Das Blockchain. Trading access and other services are provided to all account holders.

KYC & AML (Know You Customer & Anti-Money Laundering)
Each DasWallet account must be registered to a person or entity, with corresponding KYC data provided prior to the account being fully operational. This way, the entity providing DasWallet services can comply with applicable regulations. The DasWallet system requires account holders to be identified and in good standing before engaging in activities within the system. This type of authentication protocol results in a higher level of integrity amongst participants.

External Exchanges
Additional access points for handling digital assets from the Das Blockchain include a number of public cryptocurrency exchanges. Trading under the symbol of DASC, DasCoin can be purchased, sold and held in accounts through these exchanges. All of the exchanges that currently list DasCoin have KYC requirements that must be complied with before an account can be activated.
Blockchained Internal Exchange

The Das Blockchain also incorporates a decentralized exchange that trades, settles, and clears over the Blockchain autonomously. DasWallet account holders also have the option to transfer their digital assets to custodial accounts in centralized exchanges in order to trade.
The Network

The Board
The Das Blockchain enables a governing board to regulate the parameters of the network. The Board will be comprised of members nominated and appointed by the Board Chairman. 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.
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 Das 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. Directors can serve terms of 2-6 years. A minimum of 3 Directors are required for the governance of digital assets on the Das Blockchain, and as many as 9 may serve on the Board.

In addition, the Board structure has been designed to feature the role for an Ombudsman who is unable to vote and does not hold any responsibilities within the Board, but who can attend all Board meetings and provide 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, unless during a crisis when an additional vote is required in order to satisfy the condition of three votes. The Executive Director is responsible for directly overseeing all Chain Authorities.
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 programmed 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.
The Network

Operations
The Board sets the procedures and ensures the proper execution of the following: 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 under the supervision of the Executive Director.

Global Parameters
Listed below is the set of parameters that the Board can propose changes upon:
The Network

**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 3 seconds. In the future, this will be decreased as the code base is further optimized.

**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.

**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.

**Token Creation**
The Board has the capacity to designate the parameters for creating and issuing derivative utility tokens on the Das Blockchain.

<table>
<thead>
<tr>
<th>Account hash/name length:</th>
<th>between 3 and 63 characters</th>
</tr>
</thead>
<tbody>
<tr>
<td>Transaction size:</td>
<td>1024B</td>
</tr>
<tr>
<td>Time between blocks:</td>
<td>3 seconds.</td>
</tr>
<tr>
<td>Time between maintenance intervals:</td>
<td>1 day</td>
</tr>
<tr>
<td>Maintenance duration (# of blocks skipped):</td>
<td>3 blocks</td>
</tr>
</tbody>
</table>
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 Das 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 other assets). 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 Das Blockchain is 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 Das Blockchain is a cryptographically linked series of blocks. These blocks establish a permanent record of transactions 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.

The purpose of the 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 with full access to active Ledger Nodes within the system and complete transparency regarding overall operations of the Das Blockchain.
There are inherent efficiencies to the Proof of Authority consensus model. Rather than incur the financial burden of protecting an openly-configured network of peer-to-peer servers, the Das 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 in the operation of its consortium of network nodes, while preserving open-system dynamics in other aspects of the system, the Das Blockchain is able to benefit from the advantages of blockchain protocol without the burden of the inefficiencies associated with decentralized open-system architecture and without the security concerns of centralized systems.
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 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 within the Das 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.