

# White Paper

VERSION: 01

RELEASE DATE: 03 OCT, 2022



This document highlights brief insight into iTachyons Neural Network technological specifications, technical strategy, applications & objectives.

[www.iTachyons.io](http://www.iTachyons.io)

**Prepared by  
Laura Samsun**

**“A first of its kind EVM compatible decentralized Proof of Authority blockchain with support for private and anonymous transactions and sealing rewards.”**



## **What is the iTachyons Blockchain?**

iTachyons is a revolutionary EVM compatible decentralized Proof of Authority blockchain with support for private and anonymous transactions, on-chain governance and sealing rewards. It is the first of its kind to enable developers to quickly and easily deploy and manage their own decentralized applications (dapps) in a PoA ecosystem. Tachyons unique consensus algorithm enables high performance, low latency and secure transactions, making it the perfect platform for a wide range of use cases, from gaming and communications, to digital currencies and digital assets. Tachyons, supervised by the Tac Foundation Group, is committed to the highest standards of security and transparency, and is designed to provide an easy and intuitive user experience.

## **Privacy issues with existing Blockchains**

1. **Lack of Privacy:** Most existing blockchains are public and transparent, meaning that all transactions are visible to anyone on the network. This lack of privacy can be a major concern for users who wish to keep their transactions private.
2. **Security Risks:** Blockchains are vulnerable to hacking, as they are decentralized and open source. This means that malicious actors can exploit weaknesses in the system to gain access to user data or funds.
3. **Scalability Issues:** As blockchains become more popular, they can become congested and slow. This can lead to delays in transactions and higher fees.
4. **Regulatory Uncertainty:** Governments and other regulatory bodies are still trying to figure out how to regulate blockchains and cryptocurrencies. This lack of clarity can make it difficult for businesses to operate in the space

## **Privacy with the iTachyons Blockchain**

The iTachyons blockchain was built with privacy in mind and our technology and solutions assert the same mindset, while being a decentralized and public blockchain similar to the existing ones out there, we have made the following our priority:

1. **Implement Privacy-Preserving Protocols:** Privacy-preserving protocols such as zero-knowledge proofs and ring signatures can be used to ensure that data stored on a blockchain is kept private.
2. **Use Encryption:** Encryption can be used to ensure that data stored on a blockchain is kept secure and private.
3. **Utilize Private Blockchains:** Private blockchains can be used to ensure that only authorized parties can access the data stored on the blockchain. We achieve this by offering Enterprise Level permissioned blockchains, more details later in this whitepaper.
4. **Implement Access Controls:** Access controls can be used to ensure that only authorized parties can access the data stored on the blockchain.
5. **Utilize Smart Contracts:** Smart contracts can be used to ensure that data stored on a blockchain is kept secure and private.
6. **Utilize Multi-Party Computation:** Multi-party computation can be used to ensure that data stored on a blockchain is kept secure and private. A blockchain which ensures the above is still prone to privacy leaks similar to how a TOR network is when its exit nodes are compromised. Tachyons Blockchain goes one step further and resolves that by ensuring that we follow a Proof of Authority (PoA) consensus algorithm and the validators, sealers and delegators on our network are identity verified.

## **What is Proof of Authority**

Proof of Authority (PoA) is a consensus algorithm that is gaining traction in the blockchain space. It is a type of consensus mechanism that is based on identity as opposed to the traditional proof-of-work (PoW) or proof-of-stake (PoS) algorithms. PoA is designed to provide a secure, efficient, and cost-effective way to reach consensus in a distributed ledger system.

The main advantages of PoA are its scalability, low energy consumption, and low cost. PoA is also more secure than PoW and PoS because it relies on identity-based

consensus. Why was Tachyons blockchain built on Proof of Authority? Proof of Authority is a consensus algorithm that is based on identity. It is a variation of the traditional proof-of-stake (PoS) algorithm. In PoA, validators are selected based on their reputation and identity. This means that the validators must be known and trusted by the network. The main advantage of PoA is that it is more secure than PoS. This is because PoA relies on identity-based consensus. This generally means that the network is as secure as the identities of the validators.

1. Establish trust and security: A proof of authority blockchain provides a secure and trusted environment for transactions to take place. It uses a consensus mechanism that is based on the identity of the validators, rather than on the amount of computing power they possess. This ensures that the network is secure and reliable.
2. Increase scalability: By using a proof of authority consensus mechanism, the blockchain can process more transactions in a shorter amount of time. This allows for faster transaction times and increased scalability.
3. Reduce costs: Since the validators are known and trusted, there is no need for expensive mining hardware or energy costs associated with proof of work consensus mechanisms. This reduces the cost of running a blockchain network.

## **Proof of Authority in iTachyons Ecosystem**

For iTachyons Blockchain, we recognized that a platform relying on the identities or good intentions of our validators is not sufficient to ensure transparency and stability, hence the Tachyon Ecosystem is supervised by the Tac Foundation Group which governs the network of validators along with other aspects of the ecosystem to ensure continued sustainable development and growth. The blockchain ecosystem as a whole is referred to as the “Dark Forest” as is evident by the recent events (Luna failure, FTX fiasco to name a few), Tac Foundation Group is created to act as the light at the end of this dark tunnel and not only be the watchdog but to active step-in and vote on matters of critical importance to ensure community value.

This brings up yet another question about how the validators or sealers are rewarded or kept honest? Our answer to this is by introducing sealing block rewards at a protocol level, every authorized PoA sealer, validator or delegator is awarded whenever a block is sealed and strict penalties exist for anyone who tries to put the system to fault or otherwise act in any way that can be seen as dishonest.

## **What are sealing block rewards in a Proof of Authority blockchain?**

Sealing block rewards in a Proof of Authority blockchain are rewards given to validators for creating blocks. These rewards incentivize validators to maintain the network and ensure that the consensus rules are followed. The rewards are typically a portion of the transaction fees collected from the transactions included in the blocks.

## **Applications of the iTachyons Blockchain**

iTachyons Blockchain has several potential applications. These include but are not limited to:

1. Supply Chain Management: Tachyons Blockchain can be used to securely and efficiently manage supply chains. This is because it is more secure and cost-effective than traditional methods.
2. IoT: Tachyons Blockchain can be used to securely manage the data generated by IoT devices. This is because it is more secure and cost-effective than traditional methods.
3. Decentralized Applications: Tachyons Blockchain can be used to securely manage decentralized applications. This is because it is more secure and cost-effective than traditional methods.
4. Private Enterprise Network: Our corporate clients can benefit from the flexibility of our blockchain by creating their own private network from the genesis block and run their own asset tracking system and other decentralized applications in a permissioned cloud.
5. Blockchain interoperability: With our cross chain contracts and EVM compatibility, iTachyons Blockchain recognizes and achieves the objective of maintaining cohesiveness and integrating with the other blockchains and decentralized applications

## **iTachyons Blockchain for Enterprises**

iTachyons Blockchain was built with privacy in mind, we recognise the importance of data abstraction and obfuscation when it comes to our enterprise clients, who want to maintain a permissioned public ledger while keeping the transactions private within their sphere.

iTachyons Blockchain uses a combination of public and private keys to ensure that only the intended recipients have access to the data stored on the blockchain. The data is encrypted and stored on the blockchain, while the public key is used to authenticate the transaction and the private key is used to decrypt the data. This ensures that only the intended recipients can access the data stored on the blockchain.

iTachyons Blockchain also offers a range of privacy-enhancing features such as zero-knowledge proofs, multi-signature transactions, and ring signatures. These features allow users to keep their transactions private and secure, while still allowing them to take advantage of the benefits of the blockchain.

### **Long Term Technical Strategy for iTachyons Blockchain**

1. Monitor and maintain the network: Regular monitoring and maintenance of the network is necessary to ensure that it remains secure and reliable. This can be achieved through the use of automated tools, manual audits, and other security measures.
2. Maintaining a decentralized and global network of validators and sealers by Providing incentives for validators and sealers to maintain the network and onboarding new network actors.
3. Off-chain Computation: Off-chain computation is a way to perform blockchain transactions without having to broadcast them to the entire network. This allows for private and anonymous transactions to take place on the blockchain. Off-chain computation can be used to create smart contracts, execute transactions, and store data securely. It will primarily be used in our anonymous transactions and permissioned enterprise private networks.

### **Cross Chain Swaps using iTachyon Blockchain**

Cross-chain swaps for EVM compatible blockchain are possible through the use of atomic swaps. Atomic swaps are a type of smart contract that allows two parties to exchange digital assets without the need for a third-party intermediary. This type of swap is possible because the two parties are able to lock up their respective assets in a smart contract and then release them to each other when the conditions of the contract are met. This type of swap is especially useful for EVM compatible blockchains because they are able to interact with each other through the use of smart contracts. This allows for the seamless exchange of assets between two different blockchains without the need for a third-party intermediary.

iTachyons Blockchain has the following Cross Chain Swaps available at the time of mainnet release

1. Ethereum <=> Binance Smart Chain
  - a. USDT
  - b. BNB
  - c. ETH

### **Private Transactions with iTachyon Blockchain**

iTachyon Blockchain is fungible because it is private by default. Units of iTachyon Blockchain (TACS) cannot be blacklisted by vendors or exchanges due to their association in previous transactions.

Zero-knowledge proofs (ZKPs) are cryptographic methods that allow two parties to prove the validity of a transaction without revealing any sensitive information. ZKPs are used to enable private transactions on public blockchains, such as the Tachyons Blockchain. ZKPs are based on zero-knowledge succinct non-interactive arguments of knowledge (zk-SNARKs). These cryptographic proofs allow Tachyons users to prove that a transaction is valid without revealing any of the details of the transaction thus maintaining anonymity.

Mixing transactions and zero knowledge snarks can be used to facilitate private blockchain transactions. Mixing is a process of combining multiple transactions into one transaction, making it difficult to trace the origin of the funds. By combining these two technologies, users can create private transactions that are secure and untraceable. This can be especially useful for businesses that need to keep their transactions private, such as those dealing with sensitive data or financial transactions.

### **What is the TAC Foundation Group?**

The Tac Foundation Group is a non-profit organization, built by the founding sealers and members of the Tachyon Blockchain, that is dedicated to advancing the development and adoption of blockchain technology. The group works to promote the use of blockchain technology to create a more secure, transparent, and efficient digital economy. The Tac Foundation Group also provides educational resources and support for developers, entrepreneurs, and businesses interested in leveraging blockchain technology.

### **What are the primary objectives of the TAC Foundation Group (TFG)?**

1. Ensure transparency and accountability in decision-making.
2. Establish clear and consistent rules and regulations.
3. Encourage collaboration and communication between stakeholders.
4. Foster trust and security in the network.
5. Enable efficient and secure data management.
6. Promote scalability and interoperability.
7. Provide incentives for users to participate in the network.
8. Support the development of innovative applications.
9. Create a platform for decentralized autonomous organizations.
10. Establish a secure and reliable infrastructure for digital transactions.

## **How does the TFG ensure the survival of the Tachyon Ecosystem?**

1. Create a Strong Foundation: Ensure that the blockchain ecosystem is built on a strong foundation of technology and protocols that are secure, reliable, and scalable.
2. Foster Innovation: Encourage developers to create innovative applications and services that can be used within the ecosystem.
3. Develop a Robust Regulatory Framework: Establish a clear and comprehensive regulatory framework that can protect users and ensure the integrity of the blockchain ecosystem.
4. Promote Adoption: Educate users and businesses about the benefits of using blockchain technology and encourage them to adopt it.
5. Establish Partnerships: Develop strategic partnerships with other industry players to create a more robust and interconnected ecosystem.
6. Invest in Security: Invest in security measures to protect the blockchain ecosystem from malicious actors.
7. Monitor and Respond: Monitor the blockchain ecosystem for any suspicious activity and respond quickly to any threats.

## **Technical Specifications**

### ***Heka - Testnet***

Chain ID: 760

RPC URL: [http://heka\\_rpc.tacscan.io:8545](http://heka_rpc.tacscan.io:8545)

WS URL: [ws://heka\\_rpc.tacscan.io:8546](ws://heka_rpc.tacscan.io:8546)

Symbol: TACS

Explorer: <https://testnet.tacscan.io>

Faucet: <https://faucet.tacscan.io>

Please make sure you are connected to the correct network in your metamask or wallet before using the faucet

*Network Dashboard: <https://stats.tacscan.io>*

### **Chain Specifications**

Total Supply: 300,000,000

Consensus Algorithm: PoA

Block Time: 3 seconds

EIP150, EIP155, EIP 158, Byzantium, Constantinople, Petersburg supported Native transfer gas requirement: 21,000



TPS: 100k

Gas Limit Per block: 34,603,008

Supports more complex smart contracts as compared to Ethereum Chain  
Tac Token Standard TTS-20 (Fungible Tokens), TTS-721 (Non-Fungible Tokens),  
TTS-1155 (Multi Tokens) supported

Uses ~ 5% of the entire energy requirements of Bitcoin

Supports the cutting edge Solidity 0.8+

### **Precompiled Contracts (For Developers)**

Address 0x01: ecrecover

Address 0x02: sha256hash

Address 0x03: ripemd160hash

Address 0x04: dataCopy

Address 0x05: bigModExp{eip2565: true}

Address 0x06: bn256AddIstanbul

Address 0x07: bn256ScalarMulIstanbul

Address 0x08: bn256PairingIstanbul

Address 0x09: blake2F

Address 0x10: bls12381G1Add

Address 0x11: bls12381G1Mul

Address 0x12: bls12381G1MultiExp

Address 0x13: bls12381G2Add

Address 0x14: bls12381G2Mul

Address 0x15: bls12381G2MultiExp

Address 0x16: bls12381Pairing

Address 0x17: bls12381MapG1

Address 0x18: bls12381MapG2

*For a complete list of precompiled contracts, please reach out to our development team*

*WBNB Contract: 0x66A2Fa2BE42ac41F0F3d254A9194E31525b50BD4*

### **Thoth - Mainnet Release**

Chain ID: 765

RPC URL: [http://heka\\_rpc.tacscan.io:8555](http://heka_rpc.tacscan.io:8555)

WS URL: ws://heka\_rpc.tacscan.io:8556

Symbol: TACS

Explorer: https://tacscan.io

Consensus Algorithm: PoA with block rewards

### ***Chain Specifications***

Total Supply: 300,000,000

Consensus Algorithm: PoA

Block Time: 5 seconds

EIP150, EIP155, EIP 158, Byzantium, Constantinople, Petersburg supported Native transfer gas requirement: 21,000

TPS: 100k

Gas Limit Per block: 34,603,008

Supports more complex smart contracts as compared to Ethereum Chain Tac Token Standard TTS-20 (Fungible Tokens), TTS-721 (Non-Fungible Tokens),

TTS-1155 (Multi Tokens) supported

Uses ~ 5% of the entire energy requirements of Bitcoin

Supports the cutting edge Solidity 0.8+

### **Block Rewards:**

3 TACs every block or every 5 seconds for 2 years = 37,872,000

1.5 TACs every block or every 5 seconds for 2 years = 18,936,000

0.75 TACs every block or every 5 seconds for 2 years = 9,468,000

0.375 TACs every block or every 5 seconds for 4 years = 9,468,000

0.1875 TACs every block till max supply hits

### **Precompiled Contracts (For Developers)**

Address 0x01: ecrecover

Address 0x02: sha256hash

Address 0x03: ripemd160hash

Address 0x04: dataCopy

Address 0x05: bigModExp{eip2565: true}

Address 0x06: bn256AddIstanbul

Address 0x07: bn256ScalarMulIstanbul

Address 0x08: bn256PairingIstanbul

Address 0x09: blake2F

Address 0x10: bls12381G1Add

Address 0x11: bls12381G1Mul

Address 0x12: bls12381G1MultiExp

Address 0x13: bls12381G2Add

Address 0x14: bls12381G2Mul

Address 0x15: bls12381G2MultiExp

Address 0x16: bls12381Pairing

Address 0x17: bls12381MapG1

Address 0x18: bls12381MapG2

For a complete list of precompiled contracts, please reach out to our development team

*WBNB Contract: 0xB3c7Ba651e78C51E0669CE891f18e8dF168837Fa*

### **Github Codes Repository:**

*[www.github.com/itachyons](https://www.github.com/itachyons)*

### **Other Websites For Reference:**

Blockchain Information: <https://www.iTachyons.io>

Blockchain Explorer: [www.TacScan.io](http://www.TacScan.io)

Tachyons Foundation Group (DAO): [www.iTachyons.org](http://www.iTachyons.org)



iTachyons



iTachyons Cohort FZC

**Thank  
You**



**Connect With Us :**

[www.iTachyons.io](http://www.iTachyons.io)

Email Address: [info@iTachyons.io](mailto:info@iTachyons.io)

Telegram: [@iTachyons](https://t.me/iTachyons)