

AUTOBAHN
NETWORK

Autobahn Network Lightpaper

Private DeFi on Bitcoin

The Autobahn Network paves the way for high-speed digital asset transactions for everyday use and protects the privacy of its users.

Autobahn Network by "Tixl gGmbH"
<https://autobahn.network>

Contact:
mail@autobahn.network

July 2020

Executive Summary

What problems does the Autobahn Network solve?

Bitcoin and many other digital asset transactions are slow, expensive and traceable. People currently value most digital assets as an investment, but not as a medium of exchange.

The Autobahn Network is a **Private Defi Platform** allowing Bitcoin, and other digital assets, to be sent quickly and privately with low transaction fees. TXL is the native token of the Autobahn Network. Transaction fees (and other network fees) are paid, indirectly, in TXL. TXL itself can be sent with zero transaction fees. In that respect, TXL has the properties of today's cash and stands apart from other digital assets.

What solution does the Autobahn Network provide?

The Autobahn Network employs the most sophisticated technologies to have emerged from the blockchain world over recent years to build a decentralized payment network. Bitcoin (and any other digital asset) can be sent to the Autobahn Network. Within the Autobahn Network, digital assets can be sent quickly, privately and with low transaction fees.

What is the current status of the project?

The Autobahn Network is still under development but has already launched a public testnet which includes all the main features and provides the ability to send Testnet-BTC between web wallets. The next steps will be to provide the ability to send real BTC and to onboard the first early adopters. More details can be found on the [website roadmap](#).

Why does a token exist if the project is under development?

We created an intermediary token on another platform before the launch of the Autobahn Network. This was done, in part, to secure the first rounds of funding for the project. Our token is based on Binance Chain and has the symbol MTXLT. MTXLT stands for "Million TXL Tokens". When the Mainnet launches, MTXLT owners will have the right to swap 1 MTXLT (Binance Chain) for MTXL / 1,000,000 TXL (the Autobahn Network).

Autobahn Network by "Tixl gGmbH"

<https://autobahn.network>

Contact:

mail@autobahn.network

July 2020

The Journey

Where have we come from?

When we started the project back in 2018, our goal was to create a private, fast and feeless cryptocurrency. We called both the project and the currency, “**Tixl**”. We worked with the BaFin (one of the toughest financial regulators in the world) to ensure our project was feasible. After getting the “green light” we began development and the fundraising. By mid-2019, we had finished our first round of seed funding, completing a token sale raising USD\$1,250,000 from retail investors.

The Bigger Picture – Recognizing the Opportunity

By the end of 2019, we realized there was a huge potential beyond simply developing our own currency. Watching the Bitcoin scaling debate, it became clear that the only way Bitcoin will scale to reach its full potential is through second-layer solutions. As a result, we designed our platform to provide the optimal properties for being a second-layer solution for Bitcoin. We evaluated the remaining technical questions and started pivoting. The era of our new platform was born: The **Autobahn Network**.

Keeping the Tixl Token [TXL]

We strongly believe in the fundamental properties of our own token – which combines zero-fees with fast and private transactions. The value of Tixl will be increased by using it as the native token in the Autobahn Network, which benefits investors. TXL will be used to cover transaction fees, pay for listings of additional assets, and for purchasing other network services (such as nicknames). We want to make the onboarding of BTC users as easy as possible – so transaction fees can be paid in BTC, which can then be used to purchase TXL tokens on the public market – thereby increasing the demand for Tixl.

Autobahn Network by “Tixl gGmbH”

<https://autobahn.network>

Contact:

mail@autobahn.network

July 2020

The Tech

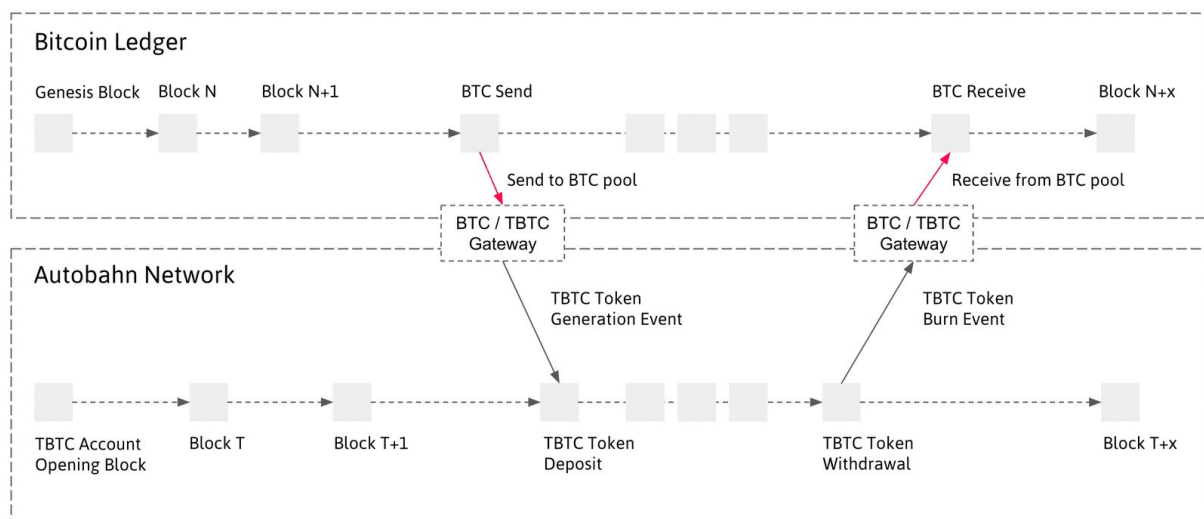
Since the Autobahn Network was born from the Tixl project, a lot of the technical details about our data structure and consensus algorithm can be found in the [Tixl whitepaper](#). The chapter below provides an overview of how our Private DeFi Platform works:

General Concept

The Autobahn Network delivers a novel way to move other assets on the network that is used by Tixl, which offers speed and privacy. In contrast to existing solutions, we do not rely on peer-to-peer payment channels, nor on centralized solutions, to swap tokens.

The basic idea involves sending the native tokens (we will use Bitcoin as the example for all assets in the following) to the address of a decentralized committee that stores the Bitcoin safely until they are withdrawn from the Autobahn Network. This is achieved by giving a subset of all validators, called “the committee” (that makes sure every transaction is legitimate), key shares to a Bitcoin account.

With these key shares, the committee can sign Bitcoin transactions in a decentralized way, without single validators being able to move Bitcoin out of the fund. For every Bitcoin deposited into the Autobahn Network, an equivalent TBTC on the Autobahn Network is created which will later be burned in the case where the Bitcoin is withdrawn. The following illustration shows how the Bitcoin Ledger is connected to the Autobahn Network via a “BTC / TBTC Gateway”:



Autobahn Network by “Tixl gGmbH”

<https://autobahn.network>

Contact:

mail@autobahn.network

July 2020

Decentralization

One of the central concerns for the second-layer solution is to enable the transfer of other assets while maintaining decentralization. This is trivial for the transactions in the network itself, as it uses the mechanisms of the existing Tixl solution - which achieves consensus using the Stellar Consensus Protocol. However, the more challenging task is to guarantee decentralization for the transactions that bring assets into the Autobahn Network (deposit), and those that take them back to their native chain (withdrawal).

The native asset can never leave the native chain, as no entity in the Tixl Network has the authority to mint or burn native assets. Instead, the solution is to transfer the ownership of the native tokens to the Tixl Network on deposit and to transfer it back on withdrawal.

To achieve this in a decentralized way, the Autobahn Network uses a Multi-Party Threshold Signature Scheme (TSS).

A subset of the validator nodes (the committee) will be chosen using criteria like global network trust and decentralization. Every member of the committee participates in the three algorithms of the TSS: Key generation, key re-sharing and signing.

From the global public key, the address, e.g. the bitcoin address, can be calculated, which is the pool address. When enough members of the committee work together they can produce a valid signature for the corresponding global private key, thus allowing the committee to spend the funds that have been transferred to the pool address.

It should be noted that no committee member reveals their key share or can produce signatures alone. The key re-sharing algorithm allows the committee to generate new key shares without changing the underlying global private key, and even allows for new committee members to enter and old ones to leave.

Autobahn Network by "Tixl gGmbH"

<https://autobahn.network>

Contact:

mail@autobahn.network

July 2020

Threshold Signature Scheme (TSS)

Since we aim to stay decentralized, no single validator should be able to spend Bitcoin from the shared pool where the Bitcoins are deposited. Therefore, a process such as using a threshold signature scheme (TSS) is needed.

A (t,n) TSS is a group of n parties sharing a secret in such a way that only $\geq t$ parties are able to reconstruct the secret respectively to produce a signature in a decentralized way, without revealing their shares. Additionally, there is a decentralized algorithm to create the secret shares without any party knowing more than its share.

The Autobahn Network "BTC / TBTC Gateway" relies on the implementation of Binance written in Go, which has been security audited and offers all the features we require.

The library offers three algorithms:

Keygen

This algorithm lets n parties create keys with a threshold of t , which can be used for the other two algorithms.

Signing

This algorithm creates a signature and requires at least t parties to participate.

Resharing

To make the storage of the secrets more secure, the secret shares can be regenerated with the underlying secret, thus allowing the Bitcoin address to remain the same. This is yet to be implemented in our Testnet.

Autobahn Network by "Tixl gGmbH"

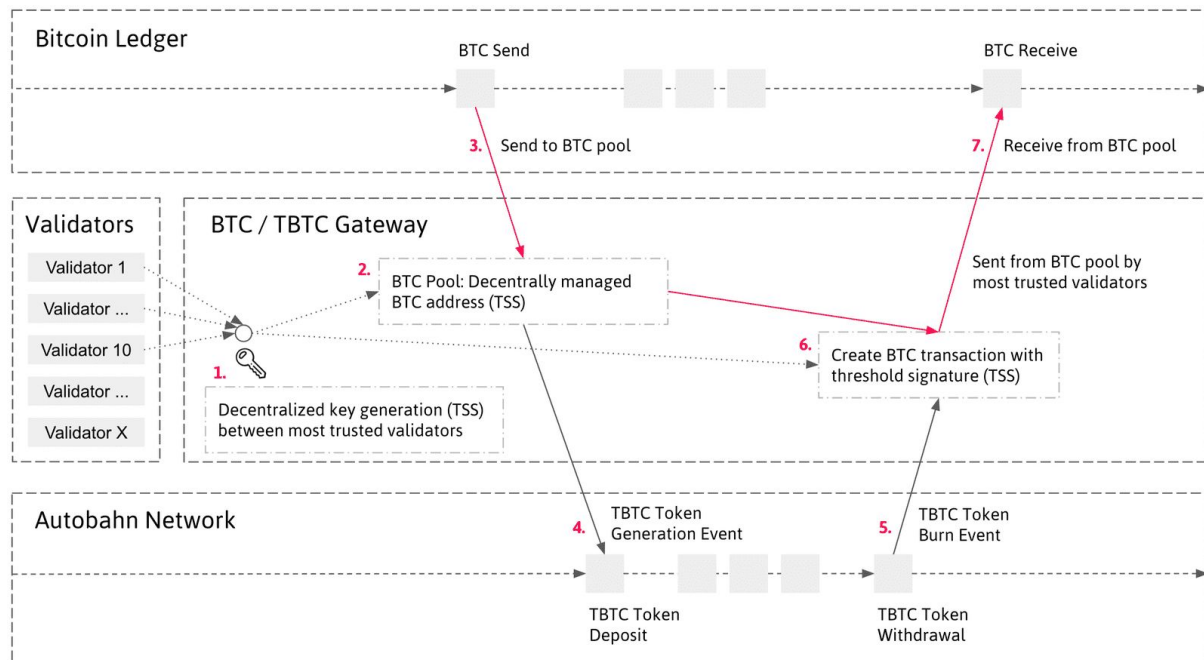
<https://autobahn.network>

Contact:

mail@autobahn.network

July 2020

Deposit



The transferring of assets to the Autobahn Network is quite simple: The user sends the amount they wish to deposit to the pool address and creates a Deposit Block, which contains a reference to the transaction of the native token, on the Autobahn Network.

To prevent any others from claiming that transaction a claim proof must be provided. Currently, two different claim proofs are implemented.

The first method to proof that the user can use the transaction for the deposit block is to sign the public key of the stealth chain the deposit block is going to be placed on with the asset private key and then supply this signature to the block. The second method is to send any amount to a second address, which is deterministically generated from the public key of the stealth chain.

In addition, the following criteria must be fulfilled by a deposit block in order to be accepted by the validators: The asset transaction must not have been used in any other deposit block before, the transaction must be confirmed (e.g. 6 times for bitcoin), the asset symbol of the deposit block must match the asset transaction, and the amount of the deposit block must match the amount that was transferred to the pool.

Autobahn Network by "Tixl gGmbH"

<https://autobahn.network>

Contact:

mail@autobahn.network

July 2020

The deposit block mints the respective asset tokens on the Autobahn Network. Thus, when the deposit block is accepted by the validator network, the token - in an amount equal to the transaction in the pool - can then be moved on the Autobahn Network, while the committee holds access to the native tokens in the pool.

Withdrawal

To withdraw tokens of an asset from the Autobahn Network, in order to receive native tokens, a withdrawal block must be created. The withdrawal block has an additional field where the address on the native chain the token should be transferred to is stored, and the amount is public.

When the address is validated, and the block itself is valid, the acceptance of the block results in a token burn of that asset. The committee witnesses the externalisation of the withdrawal block and creates a transaction of the asset type, e.g. a native Bitcoin transaction, and executes the distributed signing algorithm.

When enough committee members participate in the signing, a signature is eventually produced which is used to complete the transaction. The transaction is then sent to the native networks, e.g. Bitcoin Network, and the transaction reference is made public so that the user can retrieve it.

Note that the transaction fee of the native asset is paid from the amount withdrawn. The balance of the pool can never drop below zero because only tokens that have been deposited can be withdrawn.

Secured by Bitcoin

To increase the decentralization of Autobahn Network, a hash representing the current state of the Autobahn Network ledger will be written onto the Bitcoin blockchain on a regular basis. In doing so, the Autobahn Network will increase its trust by leveraging the most secure blockchain in the world.

Autobahn Network by "Tixl gGmbH"

<https://autobahn.network>

Contact:

mail@autobahn.network

July 2020

Chief Executives

The Autobahn Network project was initiated by the elbstack GmbH, a software development company based in Hamburg, Germany. Christian and Sebastian are managing directors and co-owners of the elbstack GmbH and founded the Tixl gGmbH as a 100% elbstack subsidiary in 2019. elbstack was built based on the vision of an autonomous organization where employees are relied on to take responsibility. This allows Christian and Sebastian to focus their efforts on Tixl and the Autobahn Network, with the management of elbstack being a side-activity. Without the combination of capital from elbstack, and the team-support, the Autobahn Network project would not have been possible. Bernd is the first elbstack employee who has transitioned to the Tixl gGmbH.

We, as the project leaders, are not the only people working on the Autobahn Network. There are a number of team members and advisors working on different aspects of the project, and they can be found on our website.



Christian Eichinger
Managing Director



Sebastian Gronewold
Managing Director



Bernd Strehl
Chief Technology Officer

Autobahn Network by "Tixl gGmbH"
<https://autobahn.network>

Contact:
mail@autobahn.network