Whitepaper

Version 1 - March 2019

Link Disclaimer

Our Whitepaper contains links to external websites. Despite our careful content control, we assume no liability for the content of external websites. We have no influence on the content of external websites and the operators of the linked websites are solely responsible for their content.

Abstract

The financial market has been undergoing a major transformation for some time now. The possibilities offered by the Internet are leading to an increasing digitalization of the traditional banking business. In particular, the start-ups in this market known as FinTechs are ensuring ongoing innovations and putting the traditional banks under increasing pressure. For online purchases, payment providers such as Stripe and PayPal have been able to establish themselves instead of traditional banks. With Apple and Google, two more IT giants are pursuing the goal of further digitizing payment transactions and making them extremely convenient via smartphones.

With the publication of Bitcoin and the invention of blockchain technology, it became possible for the first time to transmit values in a decentralized network without a central authority. The age of cryptocurrencies was born. Inspired by Bitcoin, numerous other cryptocurrencies were developed, adding new functions or improving existing protocols.

This Whitepaper explains which properties a cryptocurrency should have in order to be really suitable for everyday use. It is noticeable that so far none of over 2000 cryptocurrencies can sufficiently fulfill these characteristics.

Tixl takes up exactly this challenge and presents a technical concept and a project plan. The technical concept of Tixl is influenced by different approaches of existing cryptocurrencies. For scalability, Tixl will use a Directed Acyclic Graph (DAG) as data structure instead of the classic blockchain. This data structure is also used in a similar form for “IOTA”[1] and “Nano”[2]. Regarding the consensus algorithm, Tixl's architecture and decentralization philosophy is oriented to existing Federated Byzantine Agreement (FBA) algorithms like the ones from "Ripple"[3] and "Stellar"[4].

In addition to high transaction speed, Tixl attaches great importance to privacy. The use of stealth addresses has proven successful in protecting identity. These are also used, for example, by “Monero”[5]. In addition to identity protection, it is also important that transaction amounts cannot be viewed by outsiders. In order to achieve this, Tixl uses a special cryptosystem adapted to the goal at hand.

When designing a digital product which is decentralized and must be guaranteed to operate securely in 10+ years, the question of a protection against a possible attack by quantum computers is unavoidable. For this reason, different cryptosystems were compared for Tixl and it is currently planned to use NTRU[6] to encrypt credit balances and transaction amounts. By satisfying the need for homomorphic characteristics and the desire for secure protection against future computer developments NTRU turned out to be a possible choice for Tixl.

[1] IOTA cryptocurrency: https://www.iota.org
[2] Nano cryptocurrency: https://nano.org
[3] Ripple cryptocurrency: https://ripple.com
[4] Stellar cryptocurrency: https://www.stellar.org
[5] Monero cryptocurrency: https://www.getmonero.org
[6] NTRU cryptosystem: https://en.wikipedia.org/wiki/NTRU

Foreword

Tixl aims to develop a platform in the form of a cryptocurrency in which the cryptocurrency can cover the most important properties of classic Fiat money[7].

First, we look at the characteristics that determine the classic monetary system (in many countries around the world). With a Fiat currency such as the US-Dollar, payments can be made in two different ways:

- Cash
- Digital (by bank transfer, credit card or a provider such as PayPal)

We can observe the following properties in the payment processes:

1. Privacy: For those not directly involved, the transaction is not traceable.
2. Speed: Apart from the classic bank transfer, the transaction is confirmed within a few seconds.
3. Exemption from charges: Apart from e.g. international bank transfers or e-commerce payments, the money transfer is free of charge.

As a rule, the performance of the respective currency is controlled by a central bank of the respective country. This is precisely where the criticism raised by cryptocurrencies against the classic banking and financial system is focused. Those problems are repeatedly apparent in emerging markets where they are reflected by inflation spiraling out of control and a fall in the exchange rate of the national currency. This is currently evident in Argentina, Venezuela and Turkey, among others. But also large industrial nations can be affected, as the financial crisis triggered 2008 in the USA revealed.

The crypto revolution started with Bitcoin. Inspired by the possibilities to build a decentralized and self-sufficient network, aspects of existing solutions were improved again and again. For example, Monero is based on Bitcoin and has added privacy to it. Other solutions such as IOTA and Nano have transferred the concept to a more scalable data structure, whereby transactions are considerably faster than with Bitcoin and are also free of charge.

However, there is currently no cryptocurrency that can sufficiently fulfill each of the three observed properties. As such, Tixl will be focused to be one of the first cryptocurrencies meeting these characteristics. In order to be a hundred percent focused to the requirements as a means of payment, other popular developments for cryptocurrencies such as smart contracts or a data marketplace are deliberately avoided.

[7] Fiat money: https://en.wikipedia.org/wiki/Fiat_money

Table of Contents

1 Introduction

This document describes the process of how the cryptocurrency Tixl will be built, launched and developed over time.

1.1 Tixl Explained in 3 Sentences

The project Tixl is about creating a cryptocurrency - also named Tixl - that focuses on feeless, fast and private transactions. Tixl accomplishes this by utilizing an unprecedented mix of quantum secure cryptography, a state-of-the-art consensus algorithm, and a multi-blockchain data structure. As declared in the glossary the currency shortcode for Tixl is TXL.

1.2 Motivation for Developing Another Cryptocurrency

Over 2000 cryptocurrencies are listed on https://coinmarketcap.com/ already. Only a few of these cryptocurrencies pursue the goal of establishing themselves as an actual means of payment. A large number of them can be classified as utility tokens and offer a token for a new application on an existing platform like "Ethereum"[8]. Currently, the use of "ERC-20 Tokens"[9] on the Ethereum blockchain seems to be the most common.[10]

On the other hand, cryptocurrencies with their own technical solutions have very different focal points. In particular, the following trend topics can be identified again and again:

- Smart contracts
- Data marketplace
- Privacy
- Scalability
- Transaction speed
- Quantum resistant encryption

Due to the technical implementation of existing solutions, no cryptocurrency has yet been able to fulfill the mandatory requirements of privacy, feeless transactions and high transaction speed in a sufficiently collaborative manner. For this reason, Tixl will provide its own technical solution, which will be perfectly tailored to the focus on payments.

1.3 Tixl in Numbers

The TXL supply is limited and pre-mined. There will be 900,000,000,000 TXL (900 billion TXL). The supply can never be increased. 1 TXL has 7 decimal places so that the smallest amount of TXL is 0.0000001.

[8] Ethereum: https://www.ethereum.org
[9] ERC-20 Token: https://en.wikipedia.org/wiki/ERC-20
[10] Represents the current market at the version 1 release of this Whitepaper.

2 Initial Coin Offering (ICO)

ICO[11] is the abbreviation for Initial Coin Offering. ICOs are an alternative to classic fundraising methods and have proven themselves in recent years for projects that use blockchain or focus on decentralization.

Legal disclaimer: For all information about the ICO please also refer to the General Terms and Conditions.[12]

2.1 Why Should an ICO be Carried Out?

The development of Tixl itself is laborious. It is clear that a software development team is needed to implement the Tixl ledger step by step. Moreover, social media, accounting, legal and tax services, as well as security audits will need to be contracted.

In addition to the development, there is the cost of exchange listings. Some exchanges will probably accept Tixl without a financial contribution or in exchange for an amount in TXL itself. However, to be accepted as a cryptocurrency on the market, Tixl will have to be traded on major exchanges which frequently require payments of six-figure amounts for listings.

The hosting of Tixl nodes should be decentralized over time. In the beginning, the Tixl organization will have to provide nodes and must bear the corresponding monthly costs for computing infrastructure.

Last but not least, Tixl can only succeed if as many people as possible use TXL for their payments. There will be all sorts of marketing campaigns to achieve this. The same applies here as with the exchange listings. For some marketing campaigns (e.g. influencers or B2B partnerships), TXL may be issued, but some will require payments in US-Dollars, Euros or other FIAT currencies.

2.2 Does the ICO Consist of Different Phases?

In comparison to other ICOs having different phases like a private sale, presale and public sale Tixl keeps it simple by conducting only a public ICO. During 5 quarters starting on April 15, 2019 "Tixl Tokens" (see chapter 2.3) will be distributed at different price levels. In addition to the ICO an "Airdrop"[13] will take place and thus some Tixl Tokens will be distributed for free. To boost the marketing during the "Airdrop" a referral system will be implemented (see chapter 2.8).

The goal of the ICO is to secure the basic financing for the project. Funds raised in the ICO will be used e.g. for legal consulting, developer salaries and contracts or security audits.

The reasons for the ICO length of more than one year duration are manifold. For example, there is less dependency on a temporary bear or bull market, marketing does not have to be perfectly timed to a short timeframe, and a longer ICO will increase investor confidence as there is no attempt to collect as much money as possible in a matter of weeks.

---

[11] Initial Coin Offerings (ICOs) explained: https://www.investopedia.com/terms/i/initial-coin-offering-ico.asp

[12] Tixl General Terms and Conditions: https://www.tixl.me/legal/general-terms-and-conditions

[13] The term "Airdrop" has established itself for the free issuing of a cryptocurrency.

2.3 Is it Possible to Distribute Tixl Tokens During the ICO Although Tixl is Still Being Developed?

During the ICO, no real TXL but instead Tixl Tokens, named TXLT, on the Stellar platform will be sold. To receive the TXLT a Stellar wallet is required. These tokens are basically vouchers for TXL to be received at a later stage, as soon as Tixl Mainnet is launched (planned for Q2 2020).

After the Tixl Mainnet launch, all token holders are offered to swap their TXLT for real TXL. This method is called "Token Swap" and was also practiced for example by EOS.

2.4 Token Swap

The Token Swap will happen in Q2 2020. The Tixl gGmbH will take a snapshot of the Stellar Ledger at a previously announced time. At the time of the snapshot, every Stellar account holding TXLT will be automatically considered for the Token Swap. However, for swapping TXLT to TXL it is required that a TXLT holder confirms ownership of their Stellar account.

To confirm ownership, the public Stellar address must be entered on the Tixl account page[14]. During this process, a message must be signed with the private key of the Stellar account holding TXLT. The exact procedure will be explained, also on website, before the Token Swap.

Finally, also explained later, to receive TXL, a Tixl wallet must be created and the public address must be associated with the Stellar account, also through forms on the website.

Legal disclaimer: For more information about the Token Swap please also refer to the General Terms and Conditions.[15]

2.5 How Many TXLT Are Sold in the ICO and What Happens to the Rest?

Diagram 1 shows an overview of the TXLT distribution. It is noticeable that by far the largest part is intended for the ICO. This also includes the airdropped TXLT. The following list describes in detail how the other TXLT are planned to be used. To keep it simple, the term TXLT is used in this chapter, even though e.g. the distribution to Tixl Node hosters will happen after the token swap and thus in TXL.

[14] Tixl Website: https://www.tixl.me/account
[15] Tixl General Terms and Conditions: https://www.tixl.me/legal/general-terms-and-conditions

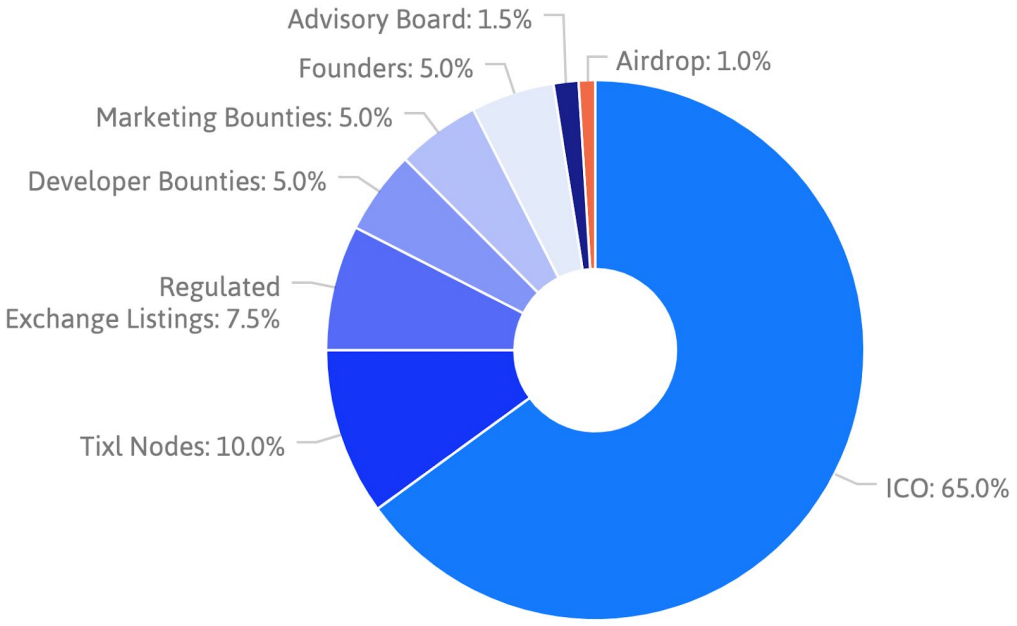

Diagram 1) TXLT distribution

ICO (65%): The by far largest amount of TXLT is offered during the ICO.

Tixl Nodes (10%): The hosting of Tixl is associated with computing power that needs to be provided by someone. Chapter 4.2.4 discusses how TXLT can be used as an incentive.

Regulated Exchange Listings (7.5%): As discussed in chapter 2.1, exchange listings are crucial to the distribution of a cryptocurrency. With this extra provision, exchanges could be offered TXLT in order to become listed.

Developer Bounties (5%): Tixl will release different parts of its software open source in the mid-term. The experience of the founding team has shown that bounties act as a catalyst when it comes to integrating external developers. For example, features of a Tixl app, or a Pay-with-Tixl integration/SDK, may be partially outsourced to external developers using bounties.

Marketing Bounties (5%): With marketing bounties, the community or B2B partners are given opportunities to perform marketing services to receive TXLT. For instance, it is considered to give an amount of TXLT to payment providers integrating and promoting payments with TXLT.

Founders (5%): The founders will finance the initial stage of the project and the preparations for the ICO. These include designs (logo, CI, documents), trademark application and legal advice being the largest expenses. Therefore the founders shall be able to buy a part of the overall TXLT supply at a lower price level.

Advisory Board (1.5%): Like almost every team working on an ICO, Tixl will have a board of advisors. Before this document was written, we held various meetings with academic advisors. Depending on the situation, there should be a small reward in the form of TXLT for this service.

Airdrop (1%): Some TXLT are given away for free (see chapter 2.7).

2.6 What Happens to TXLT Not Sold in the ICO?

TXLT not sold in the ICO will be earmarked for later sale. In turn, these will be split into 60 equal (as far as possible) packages and transferred into a 60-month escrow. Only after termination of the ICO may one of these packages be offered monthly for public or private sale. If a package is not fully sold, it will be automatically appended to the 60-month escrow again. The way this escrow behaves is pretty similar to how Ripple conducts their sales.[16]

2.7 Airdrop

To boost marketing before and during the ICO a TXLT Airdrop will start on March 18, 2019 at 12:00 pm GMT. During this Airdrop 1% of the overall TXLT supply, or in numbers 9,000,000,000 TXLT (9 billion) will be distributed free of charge. Every Airdrop participant will receive 100 TXLT free of charge. The Airdrop will either end as soon as 9,000,000,000 TXLT (9 billion) are distributed or until December 31, 2019. In case there will be any TXLT left because of too few Airdrop participants, those TXLT will also be transferred into the escrow (see chapter 2.6).

Not before January 01, 2020, airdropped TXLT tokens will be send out on the Stellar platform. This is to avoid airdropped TXLT being sold for the first period of the ICO. An Airdrop participant must store their public Stellar address on the account page until December 31, 2019 at 12:00 pm GMT. It is required that the corresponding Stellar account is activated and contains enough balance to establish a trust line with the Tixl Stellar issuer address. In case a participant does not provide a Stellar address or does not establish the necessary trust line, the accompanying airdropped tokens will also be transferred into the escrow. The Tixl Stellar issuer address will be published on the Tixl website. Also it is required, that the Airdrop participant signs a message with their Stellar private key, to confirm ownership of the Stellar account.

Nevertheless, within the Airdrop timeframe the participant will be shown a preview (on the account page) of the amount of TXLT to be received after January 01, 2020. This number can differ from the real amount of TXLT if the steps mentioned in this section are not conducted.

Legal disclaimer: Since under the Airdrop TXLT are distributed free of charge, participants do not obtain any legal entitlements or claims against the Tixl company to receive TXLT when participating in the Airdrop. In particular, please also refer to the General Terms and Conditions.[17]

2.8 Airdrop Referral Program

There will be a referral program only for the Airdrop. There will not be a referral program for the ICO as it is not the intention to create a multi-level marketing system where people buy TXLT based on emotion rather than by doing their own research. However, the Tixl Airdrop referral system has characteristics of a multi-level marketing system but as it is not required to invest money it can not be classified as a fraudulent pyramid scheme.

An Airdrop participant can refer another Airdrop participant by sending a referral link. For every referred participant the referrer will receive an additional amount of 100 TXLT.

[16] Escrow at Ripple: https://developers.ripple.com/escrow.html
[17] Tixl General Terms and Conditions: https://www.tixl.me/legal/general-terms-and-conditions

If a referred participant refers another participant the first referrer will also get some extra TXLT. This is better explained by an example. Participant A refers participant B, participant B refers participants C and D. Now the credits would be:

A = 100 TXLT for joining the Airdrop + 100 TXLT for referring B + 20 TXLT for B referring C + 20 TXLT for B referring D
B = 100 TXLT for joining the Airdrop + 100 TXLT for referring C + 100 TXLT for referring D
C = 100 TXLT for joining the Airdrop
D = 100 TXLT for joining the Airdrop

As the example calculation show participant A will get 20% of B's referral bonus, but B's referral bonus will not be reduced. The multi-level referral bonus of 20% will be halved which each level of referrals. So an example for three layers would look like:

Participant A refers participant B, participant B refers participants C and D, participant C refers participant E.

A = 100 TXLT for joining the Airdrop + 100 TXLT for referring B + 20 TXLT for B referring C + 20 TXLT for B referring D + 10 TXLT for C referring E
B = 100 TXLT for joining the Airdrop + 100 TXLT for referring C + 100 TXLT for referring D + 20 TXLT for C referring E
C = 100 TXLT for joining the Airdrop + 100 TXLT for referring E
D = 100 TXLT for joining the Airdrop
E = 100 TXLT for joining the Airdrop

The referral bonus will only be credited in case the referred Airdrop participant follows the steps from chapter 2.7 and provides an active stellar account until December 31 at 12:00 pm GMT, 2019. Until then the account page will show a preview of the possible referral bonus in case all referred participants result in active accounts. Please also refer to the legal disclaimer in chapter 2.7.

3 Organizational Form

3.1 Team

The project and the team are led by the "elbstack"[18] founders and Tixl initiators Christian Eichinger and Sebastian Gronewold. Different sales partners will focus on positioning Tixl for lucrative B2B partnerships. It is our intention for Tixl to establish itself both in e-commerce and for point of sale transactions.

For all legal matters, we work together with an international legal and tax consulting firm (> 4,500 employees). For the product development an internal team will be set up and commissioned by the software agency elbstack GmbH.

In addition, there is regular coordination with professors and recognized experts from various domains such as cryptography, security, distributed systems and other related fields.

3.2 Business Model

Since Tixl transactions are carried out free of charge, no classic business model can be identified at first glance.

Initially the organization behind Tixl will be funded by issuing TXLT as part of the ICO and the sale of TXL from the escrow.

The founders will own a stake in Tixl and are thus interested in long-term performance. To ensure long-term motivation, these TXLT, later token swapped to TXL, will have a vesting period of 24 months. They are then released for a potential sale in instalments. Also after the vesting period there will be a maximum amount of TXL that can be sold per month.

3.3 Legal Form

When selecting a suitable legal form, various aspects were taken into account. The two most important criteria are to ensure long-term decentralization and independence of the currency from individual interests. In order to achieve this, Tixl is founded as a non-profit limited liability company (German gGmbH). A transfer to a foundation at a suitable time is conceivable but not mandatory.

3.4 Trademark and Patent Rights

The term Tixl is already registered as a word mark in Germany. The trademark application is supposed to prevent competing products from using or misusing the name Tixl for their own purposes.

There are currently no patent registrations. However, patent filings are not ruled out in the future. Interesting topics could be for example, specific concepts in cryptography and the consensus algorithm that distinguish Tixl from established cryptocurrencies. Patents first and foremost protect all Tixl investors, as they prevent easy knockoffs or cloning of the Tixl system.

[18] elbstack GmbH website: https://www.elbstack.com/en/

Centralization is frequently quoted as a criticism against patent applications. For instance, at some point it could happen that the community advocates an opinion on the development of Tixl, which diverges greatly from the opinion of the Tixl organization. In this case, the community could not just start a new project based on Tixl technology - the organization would thus decide centrally.

The Tixl team recognizes the problem of centralized patents management and therefore will work on a solution during or after the launch of Tixl Mainnet.

4 Technical Concept

4.1 Data Structure

The data structure is an important basis for Tixl to achieve the desired properties; particularly the high transaction speed.

4.1.1 Which Data Structure Does Tixl Use to Persist Transactions?

The Tixl ledger is a special implementation of a "Directed Acyclic Graph"[19] (DAG). The implementation of Tixl is similar to the "Block Lattice"[20] architecture of Nano (formerly RaiBlocks). A special feature here is that every user has an own blockchain and only the owner of the blockchain can write new blocks. Because of the privacy requirements, Tixl not only has one blockchain per user like Nano but instead even multiple blockchains per user depending on the amount of transactions.

4.1.2 How Much Memory is Needed per Tixl Transaction?

For a Tixl transaction, multiple blocks are generated. Currently, the required storage space of a block cannot yet be quantified exactly. Even an estimation would be too vague at this point. The cryptocurrency Nano shows that it is possible to save transactions with an average size of approx. 400 Bytes in a block-lattice architecture[21]. Due to the cryptographic requirements, Tixl transactions are expected to consume slightly more storage space.

The memory problem in the context of scaling is discussed in more detail in chapter 4.2 of the Consensus.

4.1.2 Is a Tixl Transaction Really Instantaneous?

Essentially, the Tixl data structure allows instantaneous transactions. Senders and receivers can write the transaction on their own blockchains without having to wait for other transactions on the network. Nano advertises exactly these "Instant Transactions". However, it should be noted that the recipient must be online if the transaction is to be written to the recipient's blockchain immediately after submission. If we imagine a future where people keep their funds on exchanges or banks we can assume that those managed wallets would be online most of the time.

In practice, however, this looks different. Finally, as a Tixl receiver, one cannot rely on a Tixl transmitter not being an attacker trying to manipulate the system. Consequently, as a Tixl receiver, one needs a decentralized validation system whereby one can ask if a transaction is correct. This

[19] Directed Acyclic Graph: https://www.forbes.com/sites/shermanlee/2018/01/22/explaining-directed-acylic-graph-dag-the-real-blockchain-3-0/
[20] Block Lattice: https://github.com/nanocurrency/raiblocks/wiki/Block-lattice
[21] Nano Whitepaper: https://nano.org/en/whitepaper

validation takes time because the decentralized entity must decide on a consensus relevant to the validity of a transaction. Even if this is executed within a few seconds, Tixl envisions additional mechanisms of trust to further accelerate transactions (to be announced later).

4.2 Consensus

The Tixl Consensus algorithm determines which Tixl transactions are valid and which must be discarded.

4.2.1 What are Tixl Nodes and the Tixl Network?

A Tixl Node is a computer running the Tixl server software. Since the Tixl server software will be available as open source in the mid-term, a Tixl Node can be executed by any natural or legal person without permission. Together all nodes form the Tixl network.

Nodes are needed to perform Tixl transactions in general. They ensure that a payment is transmitted from the sender to the recipient. In addition, they save the history of all Tixl transactions. Otherwise, transactions would only be stored on the sender and receiver devices and would be lost if these devices were lost.

An essential further task of the nodes is the validation of transactions. Of course, a transaction may only be written into the global transaction ledger if it is valid. An invalid transaction may be due to software errors (e.g. in a Tixl app) or sent by malicious users in the network. In this case, the nodes apply a special consensus algorithm.

4.2.2 How do the Tixl Nodes Reach a Consensus?

Many of the existing consensus approaches, like "Proof of Work" (PoW)[22] or "Proof of Stake" (PoS)[23] are not suitable for use within Tixl. Proof of Work uses too much energy and is too slow. Proof of Stake makes no sense without having inflation or transaction fees.

On the other hand there are some existing consensus algorithms that fit better to Tixl. E.g. the Consensus protocols from Ripple and Stellar would be a good alternative for Tixl. As these algorithms work on different data structures and include small transaction fees, only the way of finding consensus is interesting for a potential usage in Tixl.

The topic consensus will gain more and more focus of the team as soon as the underlying data structure is implemented. Also refer to the roadmap (see chapter 5) for a rough timeline.

4.2.3 Does Every Tixl Node Need to Know All Transactions?

A Tixl node can be operated with different configurations. Either a node stores the entire ledger (Historical Node) or a clean history that contains only the most recent transactions of the blockchains of the last active Tixl users (Present Node).

The reason for having two different types of nodes lies in the massive storage requirements as the number of transactions increases. For example, if the consumption for a transaction was 1 kilobyte, the total ledger would already be 100 gigabytes with 100 million transactions.

---

[22] Proof of Work (PoW) Consensus Algorithm:
https://www.binance.vision/blockchain/proof-of-work-explained
[23] Proof of Stake (PoS) Consensus Algorithm:
https://www.binance.vision/blockchain/proof-of-stake-explained

As part of the Tixl Node Incentive Program, Historical Nodes will receive compensation in TXL for their computing services.

4.2.4 What is the Tixl Node Incentive Program?

It is safe to assume that in the start phase of the project the motivation to host a Historical Tixl Node will be rather low. To boost the community, a number of TXL will be reserved. The reserve can then be issued in small batches to Tixl Node hosters. In the long term, Tixl will bank on a similar philosophy as Ripple. It should create an intrinsic motivation for larger TXL owners to secure their assets by hosting a Historical Node, as this in turn contributes to the stability of the Tixl network.

4.2.5 Will Tixl be 100% Decentralized from the Very Start?

Tixl's main focus is on usability, widespread and protection of investors. To achieve these goals, the system does not have to be completely decentralized from the very start. Of course, we do not want to lower the importance of decentralization with this step. However, achieving key goals is more crucial to the project than decentralizing right from the initial launch. The final decision on the degree of initial decentralization also depends on the implementation of the consensus algorithm.

Nevertheless, it is one of Tixl's top priorities to become a 100% decentralized cryptocurrency as soon as possible.

4.3 Cryptography & Privacy

Tixl is not the first cryptocurrency to address the need for privacy. The fact that privacy is an important topic in the area of cryptocurrencies is shown by the number of popular privacy coins currently on the market. Among the top 30 cryptocurrencies alone, Monero, Dash, Zcash, Bytecoin and 0x, for example, focus on private transactions. However, all existing solutions on the market have some weaknesses.

4.3.1 Motivation for Privacy

The possibilities for the transfer of payments within business environments, as well as private life, are indispensable. This is illustrated by the following two examples of trading scenarios.

4.3.1.1 Example: Sending Money Among Friends

Alice and Bob go to a burger restaurant together. Bob does not have cash on that day, and the restaurant does not accept cryptocurrency or credit cards. So Alice takes over the whole bill first and Bob owes her €15. Both are enthusiastic about cryptocurrency and want to pay the amount owed in this way.

Both have similar requirements:

- Alice does not want Bob to be able to see other transactions, or the current balance, on her blockchain.
- Bob doesn't want to pay fees to send money to Alice.

So both want cryptocurrency to function as if €15 had been handed in cash or sent via Paypal.

4.3.1.2 Example: Point of Sale & E-Commerce

Alice and Bob go to a burger restaurant together. As a hip restaurant, cryptocurrency is already accepted as a means of payment. Both the restaurant operator and the customers have different requirements for cryptocurrency:

- Payments should be completed quickly (within a few seconds).
- The restaurant does not want Alice and Bob to see payments made by other customers.
- The restaurant does not want to pay fees or at least the fees should be very low.
- Alice and Bob do not want the restaurant to be able to view other transactions in the blockchain.

The restaurant, just as Alice and Bob, wants the cryptocurrency to behave as if the bill had been paid in cash or via credit card.

In the case of non-private cryptocurrency such as Bitcoin, the competition can view all transactions to the blockchain address of a competitor and draw appropriate conclusions such as:

- How many different customers pay with Bitcoin?
- How often do these customers buy?
- Are there customers in common because both companies have been paid by the same Bitcoin address?
- How many Bitcoins does the competitor have at the moment and how quickly, or regularly, are these Bitcoins exchanged in a fiat currency? As a result, it may even be possible to draw conclusions about liquidity.

Of course, there might be mixing services or payment providers optimizing the privacy of merchants in existing cryptocurrencies. Nevertheless, as one of the latest Amazon patents[24] shows - an open data structure, not having privacy in its core, opens the door for companies being interested in payment data.

4.3.2 How Does Tixl Achieve Private Transactions?

With Tixl, private transactions are achieved by combining different approaches. First of all, a TXL owner must be protected so that nobody can see their balance. Therefore, TXL are not written to the personal blockchain (personalchain) of a user but instead to unclassifiable blockchains (stealthchains) only known by recipient and sender. The other way around, a TXL sender must also be protected so that nobody can see their outgoing transactions. This can be achieved by sending TXL directly from stealthchains that a new recipient can not relate with other TXL owners.

The Confidential Transactions section explains how it is possible for the amount of a transaction, as well as the balances on the accounts, to remain “invisible” for anyone other than the owner, and at the same time, still possible to be processed and validated by a decentralized consensus algorithm.

4.3.2.1 Personalchain

The personalchain represents the user's main account. Stealthchain references are stored in an encrypted form on this account.

[24] Amazon Streaming Data Patent: https://www.allaboutipblog.com/2018/05/the-bitcoin-implications-of-amazons-new-streaming-data-patent/

4.3.2.2 Stealthchain

A stealthchain is a separate blockchain that works much like a Monero stealth address[25]. For each sender/receiver combination, a new stealthchain is generated with the first transaction. Other blocks of the same sender are written to the same stealthchain by the receiver.

The generated address cannot be found out by a third party, even if the third party knows both participants of the stealthchain transaction.

4.3.2.3 Confidential Transactions

The goal of confidential transactions[26] is that both the amount transferred, as well as, the account balance remain untraceable to outsiders. This is made possible by generating commitments for the values. The commitments have the ability to perform arithmetic operations (addition and subtraction). So if a commitment to the number three (3) and a commitment to the number five (5) is summed up, that sum is the same as a commitment to the number eight (8). Since a commitment to a number always yields the same result, it would be quite easy to recognize the different amounts corresponding to the commitments and the transaction details would no longer be secret. Therefore, the additional use of so-called blinding factors is necessary.

The blinding factors allow for a variance for each commitment without lifting the arithmetic properties. The team has already developed a sample application for technical feasibility analysis with confidential transactions and blinding factors for the desired data structure.

4.3.3 Quantum Security

In a world of technological competition and innovation, we strive to be at the top level of modernization and advancement and provide a product, technically strong and secure enough to endure into the future.

The cryptographical aspects of the currency are no exception to this. Cryptography is a fast-changing science, where new algorithms are discovered and old ones become obsolete every year. But to everyone even vaguely familiar with the current topics of cryptographic debates it is clear, that a great challenge looms ahead – the advent of Quantum computers.

The concept of quantum computers have existed for a long time, but in recent years some of the tech giants have started to finally make practical progress on them. And while the advent of a practical, usable, functioning, well-programmed quantum computer might be decades in the future, it already stirs the waters of the cryptographic community. As usual, humanity's ideas go way ahead of the practical implementation and years before anything related to quantum computers became a reality, Peter Shor invented an algorithm (named, of course, Shor's algorithm), which uses the suspected power of a quantum computer to solve the factorization problem (if you have a number, how to find its prime factors - especially hard when the number is the product of the multiplication of two very big prime numbers).

Many of the cryptosystems currently used, like the all-prevalent RSA are directly based on factorization, many others like ElGamal and most of the elliptic curve cryptography can be reduced to a similar problem and are also solved theoretically using Shor's algorithm. Almost all digital

[25] Monero StealthAddress: https://getmonero.org/resources/moneropedia/stealthaddress.html
[26] An investigation into confidential transactions: https://github.com/AdamISZ/ConfidentialTransactionsDoc/blob/master/essayonCT.pdf

signatures are also not secure anymore. And now when quantum computers are slowly but surely becoming a reality – the world needs to change. It does not actually matter if they will come in 10 years (as the boldest predictions see it) or in 15-20 (the more realistic prognosis), and it does not matter that the change will come slowly and that even with state of the art quantum computer it will take a considerable time for it to decode any particular data, anyone who wants to stay ahead of those developments should act now.

Thus, we have decided, that in order to provide the highest quality standard of encryption and to create an enduring system, we must use cryptography that is strong against quantum computers.

4.3.3.1 Quantum Security in Tixl

Tixl uses cryptography in different parts of its software. Of course, signing transactions itself and encrypting transaction content requires cryptography. On the other hand, the consensus algorithm uses signing and encryption methods as well. Though the consensus algorithm might be upgraded to a quantum secure, later on, the Tixl ledger must be quantum secure from the beginning. To be a little bit more precise: A quantum secure signature algorithm and a quantum secure encryption/decryption algorithm are needed. For the signature part XMSS is considered, for the encryption/decryption part NTRU seems to be a good fit.

4.3.3.2 NTRU

NTRU was created in 1996 by Jeffrey Hoffstein, Jill Pipher and Joseph H. Silverman and patented one year later by NTRU Cryptosystems Inc, a company the three inventors established with Daniel Lieman. The name they gave the new system stands for “N-th degree Truncated polynomial Ring Units” (NTRU). The NTRU cryptosystem consists of two main algorithm categories: NTRU for encryption and NTRU for digital signatures, however only the encryption part is currently of interest to us. In the beginning the new cryptosystem was praised for its speed and efficiency, however there were some worries that for smaller N (degree of the polynomial) some attacks performed well. With the possible advent of Quantum computing however NTRU drew new attention and the different attacks were studied much better. A greater scrutiny upon the possible values of the parameters proved certain rings to be weaker and others to be more robust and some provably secure versions were created as soon as 2013. As of 2017 NTRU entered public domain and is free to use by anyone. Currently NTRU has been entered into the Post-Quantum Standardization Project of the US National institute of Standards and Technology.

4.3.3.3 XMSS

XMSS - standing for Extended Merkle Signature scheme, is currently one of the best candidates to become the quantum secure digital signature of the future. Its main strength lies in the fact that its security depends purely on the properties of the underlying hash functions and not on some unsolved mathematical problem, which means that there is no chance someone will someday discover a solution to that problem which will compromise the security of the signatures. It is quantum secure and no developments in quantum computers will ever challenge it. Hash-based signatures combine a one-time signature scheme with a Merkle tree structure, which adds the hash functions in such a way as to allow a very large but fixed number of multiple signings. XMSS is a further development of this concept adding pseudo random key-generation for every single signature, which needs a different private key. This makes XMSS also forward-secure which means that even if a secret key is compromised, all previous signatures remain valid and are not compromised.

5 Launch Roadmap

The development of the elementary Tixl software parts has already begun with version 1 release of this Whitepaper. At first the cryptosystem will be developed as it's the most crucial software part. Plan is to bring properly encrypted transactions onto the data structure already in Q2/Q3 2019. Starting from that point, several security audits are planned to ensure that there are no critical bugs in the cryptosystem. The number and timing of audits is tied to the funds raised during the ICO.

After focussing on the cryptosystem and data structure the team will switch to implementing the consensus algorithm in Q3/Q4 2019. As far as possible and especially for the consensus algorithm, it is planned to use and customize existing open source algorithms instead of reinventing the wheel. Parallel to the consensus algorithm development, a part of the team will start to implement a client wallet software, also based on existing open source work and depending on the consensus algorithm.

It is planned that 2020 will start with a beta test resulting in bug fixes and optimizations through Q1 2020. The goal is to launch Tixl Mainnet in Q2 2020.

5.1 Open Source

As of now it's planned that all of Tixl's software parts which are required to run and operate the network will be released open source in the mid term. Why are they not released open source straight from the beginning? The main reason is that it opens up possibilities for competitors to copy Tixl. Of course that can (and probably will) happen at a later stage as well. However, the probability that a competitor can successfully copy the system is much lower if Tixl is already in use by many users at this time. Furthermore, this also protects our investors.

5.2 Marketing Before Launch

Like mentioned earlier, success of a cryptocurrency project in 2019/2020 will most likely depend more on the marketing than on the best technical implementation. That's why the Tixl team will invest a lot of work into marketing already during the development phase. The main target group of marketing will be B2B partnerships. Existing firms in the cryptocurrency space, especially payment providers, exchanges or consulting companies already have numerous customers and can act as a catalysator for the spread of Tixl.

5.3 Updates / Communication

To always stay up to date please join our Discord[27] server at https://discord.gg/dzVzMdp

[27] Discord is an online messaging platform: https://discordapp.com

6 Risks

The risks listed below represent the risks considered material at the time this document was prepared. All risks presented individually can also occur cumulatively or to a particularly high degree and thus reinforce the negative effects on the Tixl project and the respective buyer. General negative circumstances, such as a global financial, currency and/or economic crisis, may also occur and intensify the risk consequences.

The personal and economic circumstances of a buyer cannot be taken into account below and can lead to individual risks for the buyer in question and/or increase the risks listed below.

No statement can be made as to the probability that the risks described below will occur. Nor is the order of the risks presented below a measure for their probability of occurrence or for the extent of their potential impact. For the sake of clarity, the following presentation is thematically structured, whereby it must be noted that the risks mentioned may also have cross-thematic relevance and/or may affect the occurrence and intensity of other risks.

Irrespective of the risks described here, developments that are unknown and/or unforeseeable today may have a negative impact on the Tixl Project.

The risks described below may cause the value of the Tixl Token (TXLT), but also later the Tixl itself (TXL), to develop negatively and lead to a partial or complete loss of the invested capital for the buyers.

6.1 Technical Solution

The implementation of Tixl is based on existing technologies. Which, amongst others, include: Programming languages, frameworks, network protocols, cryptographic systems and consensus algorithms. It cannot be ruled out that there may be security gaps, or other errors, in the applied technologies used or faulty compilations thereof. While this may be counteracted by the implementation of security audits, for example, there is no one hundred percent certainty in computer science and cryptography. Specifically, two scenarios in particular would have drastic effects on the Tixl price.

Scenario 1 would be a breakup of the cryptographic system. In the worst case, an attacker could thus send any number of Tixl. This would very likely make the currency worthless or at least lead to a long-term price collapse.

Scenario 2 would be a long-lasting "DDoS attack" paralyzing the Tixl network for days and for which no immediate solution could be found. Again, a long-term price collapse would be feared.

Advanced technical precautions are taken to safeguard against both scenarios thereby counteracting them and minimizing this likelihood.

6.2 Marketing & Dissemination

As mentioned numerous times, the success of a cryptocurrency depends on its dissemination. Theoretically it could happen that the implemented marketing measures show no effects and no users and B2B partnerships are able to be generated. In this case, the corporate capital would eventually

come to an end thus rendering Tixl marketing financially impossible. This would probably lead to a long-term, and rather slow, drop in price.

6.3 Regulation

Of course, governments or state institutions, whether in Germany or elsewhere in Europe, must and will deal with cryptocurrencies in the coming years. This will lead to more regulation in the relatively unregulated market. The founding team is very open to cooperation with the German state as well as other states. Tixl should definitely not become an "underground currency" but comply with the regulations set forth in public policy, provided these do not completely block the Tixl core concept. The worst case would be that states prohibit the use of Tixl as a means of payment. Depending on which state(s) is/are concerned, a ban may lead to a short-term or long-term dip in the price.

6.4 Competition

Currently, various teams worldwide are working on the implementation of a new generation of cryptocurrencies. Some startups have also recognized that the cryptocurrencies of 2019/2020 need to be more usable and that distribution is of utmost importance. There is no denying that the competition is strong and that in 2019/2020 at least 100 new cryptocurrencies will hit the market. However, the founding team is not aware of any competitors which implement the Tixl concept in a comparable way.

Of course, the usability of existing cryptocurrencies will also improve, and distribution will increase. The key currency is likely to remain Bitcoin. As in the past, the next crypto-bull market will favor the competitive drive and growth of new cryptocurrencies. On the other hand, getting started as a new Altcoin will be much more difficult in just a few years.

6.5 Key Individuals Risk

The development and economic success of the Tixl project depends to a large extent on the experience and competence of a small group of people, in particular Christian Eichinger, Sebastian Gronewold and other key people. There is a risk that these key persons may not be available or not perform their tasks (fully or properly) and that the development or economic success of the Tixl project may deteriorate or even be terminated. There is also the risk that a successor cannot be found in the event of the loss of a key person.

6.6 Risk from Conflicts of Interest

There are personnel and capital links between the partners involved in this ICO project. Participating partners and consultants are not subject to a non-competition clause. Therefore, it can not be ruled out that the partners involved as well as the persons associated with them will carry out further projects with similar criteria in the future. Irrespective of this, there is a risk that the participating partners will take measures or refrain from necessary actions due to their own or external interests and/or that decision-making situations will be resolved to the detriment of the Tixl project.

6.7 Insolvency Risk / Lack of Deposit Protection / No Capital Guarantee

The business activities of Tixl gGmbH represent an entrepreneurial commitment involving all risks of participation in business transactions. A company is always exposed to the risk of insolvency. Under no circumstances does Tixl gGmbH offer a capital guarantee. Due to lower income and / or higher

expenses, Tixl gGmbH may become insolvent or over indebted. Tixl gGmbH does not belong to any deposit insurance system. In the event of insolvency, the project cannot be realized.

6.8 No Guarantee of Tradability

TXL and TXLT should be tradable on regulated exchanges. In addition, there are no restrictions on the transfer or sale of TXL or TXLT. On the other hand, it is not possible to return the TXL or TXLT to the Tixl gGmbH. There is a regulated exchange-like market for the sale of the Tixl Token. However, there is no guarantee that the sale will be possible at all, at the desired time or at conditions acceptable to the original purchaser.

6.9 No Right to a Say

The Tixl Token is not a security; it does not convey any claims under the law of obligations or company law for co-determination and/or profits with regard to the Tixl Project and/or Tixl gGmbH. It is therefore possible that the management will make decisions which do not correspond to the objectives of the individual buyers of the TXLT and which may have a negative effect on them.

6.10 Contract Performance Risk (Counterparty Risk)

The Tixl project is based on various contractual relationships that have already been established or are yet to be established. There is a risk that the contractual partners will not meet their obligations arising from the contracts (intentionally or negligently) or will no longer be in a position to duly fulfil the contract or pay damages due to a deterioration in their creditworthiness or the accumulation of obligations towards a large number of contractual partners or will terminate their contracts properly or extraordinarily. Any claims for damages against these contractual partners may prove to be economically unenforceable and/or the necessity may arise to conduct time-consuming and costly legal disputes. This can lead to costs in connection with the enforcement of a contract or a replacement of the contractual partner. In addition, the assertion of claims for damages may be made more difficult by limitations of liability in the contracts to the extent customary in the market, and the outcome of legal proceedings and the success of enforcement measures cannot be foreseen. Any claims for damages against contractual partners due to violation of their contractual obligations may for these reasons not be (fully) enforceable. Furthermore, there is the risk that the contractually owed but not performed services cannot be procured elsewhere on the market or only at worse conditions. It must also be taken into account that the proper execution of these contracts is dependent on the economic performance and compliance of the contractual partners, the effectiveness of the individual contractual provisions and in part on the interpretation of the contractual provisions, whereby these factors may result in disruptions to the performance of the respective contractual relationships.

6.11 Reputational Risk

It is possible that the reputation of FinTechs, (large) cryptocurrencies as well as ICOs may deteriorate with individual interest groups or in society as a whole, e.g. due to a large number of unrealised projects, fraudulent or other erroneous behaviour or serious technical inadequacies (e.g. security gaps, hacks, data loss). As a result, but also as a result of corresponding events at the company level, the reputation of the Tixl gGmbH in terms of performance, competence, integrity and creditworthiness can also suffer. A deterioration in the company's reputation typically has a detrimental effect on the customer base and the company’s business actions.

Glossary

Tixl
The project and the technical execution to send and receive TXL free of charge, privately and instantaneous.

Tixl Ledger
The ledger contains the entire transaction history generated with Tixl.

Tixl Mainnet
The network of all Tixl Nodes establishing the consensus.

Tixl Node
A server running the Tixl software participating in the consensus algorithm.

TXL
TXL is the unit used in Tixl. TXL is also supposed to be used as symbol on exchanges.

TXLT
TXLT stands for “TXL Token” and describes the Token issued under the ICO.