Whitepaper

Version 4 - May 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. Unless otherwise noted, the last access was on May 1, 2019.

Executive Summary

What is Tixl?
Tixl is a new cryptocurrency that allows private, instant and zero-fee transactions.

The Problem
None of the current cryptocurrencies allows private, instant and zero-fee transactions at the same time. But why is that a problem? In a world heading more and more towards digital currencies each day, we must secure that the essential properties of traditional money preserve. Nobody, neither governments or companies nor private people want the public to be able to see all of their monetary transactions. Also, all users of a digital currency wish to pay as low fees as possible, the higher the fee, the lower the potential for widespread usage. Last but not least, if a future currency is slow, it's not a future currency.

The Solution
Tixl uses the most sophisticated technologies emerged from the blockchain world of the past years. As such, it uses a Directed Acyclic Graph (DAG) as a data structure together with the Stellar Consensus Protocol (SCP). To ensure that transactions stay private, a quantum secure cryptosystem is implemented to encrypt transaction details.

Fundraising
To finance the implementation of Tixl and also to raise capital for marketing an Initial Exchange Offering (IEO) is conducted. Even before the IEO, there will be a Pre-IEO in the form of an Initial Coin Offering (ICO). During the fundraising Tixl Tokens [MTXLT] on the Stellar platform are sold that operate as vouchers and will later be swapped to the Tixl currency itself.

Investment Potential
Similar opportunities apply to an investment in Tixl as to an investment in Bitcoin, Ethereum or another cryptocurrency. If Tixl rises in price and you bought early in the token sale, you benefit from the corresponding performance.

Legal disclaimer: There is no guarantee that an investment in Tixl will increase in value.

Foreword

Tixl aims to develop a platform in the form of a cryptocurrency in which the cryptocurrency can cover the essential properties of classic *Fiat money*[1] to be suitable for everyday use.

First, we look at the characteristics that determine the traditional monetary system (in many countries around the world). With a Fiat currency such as the USD, payments happen in two different ways:

- Cash
- Digital (by bank transfer, credit card or payment providers such as PayPal)

We can observe the following properties in the payment processes:

- Privacy: For those not directly involved, the transaction is not traceable.
- Speed: Apart from the classic bank transfer, transactions get confirmed within a few seconds.
- 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 central bank of the respective country controls the performance of its currency. The negative effects of this control results in criticism raised by cryptocurrencies against the traditional banking system. Problems with these monetary systems 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. That is currently evident in Argentina and Venezuela, 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[2] is based on Bitcoin and has added privacy to it. Other solutions 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 fulfilling these characteristics. By deliberately avoiding features like smart contracts or a data marketplace, Tixl is a hundred percent focused on the requirements of payment transactions.

[1] Fiat money: https://en.wikipedia.org/wiki/Fiat_money
[2] Monero cryptocurrency: https://www.getmonero.org

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 private and instant transactions free of charge. Tixl accomplishes this by utilizing a unique mix of quantum secure cryptography, a state-of-the-art consensus algorithm, and a multi-blockchain data structure in the form of a *Directed Acyclic Graph* (DAG). As declared in the glossary, the currency shortcode for Tixl is TXL.

1.2 Motivation for Developing Another Cryptocurrency

Over 2,100 cryptocurrencies are listed on coinmarketcap.com[3] 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*[4]. Currently, the use of *ERC-20 Tokens*[5] on the Ethereum blockchain seems to be the most common.

On the other hand, cryptocurrencies with their technical solutions have very different focal points. In particular, the following trend topics appear 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, zero-fee transactions and high transaction speed in a sufficiently collaborative manner. For this reason, Tixl will provide its technical solution, tailored to the focus on payments.

But why is failing to be private, having zero-fees and instant at the same time even a problem? Let's start with the point that the world is currently heading towards digital currencies more and more each day. All of these currencies have got the same stakeholders distributed all over the world: Governments, companies, and people. Now, if a cryptocurrency like Tixl wants to take part in the race of becoming a mainstream currency, it needs to preserve specific properties to fulfill the requirements of its stakeholders.

First of all, all of the stakeholders want the transactions made with the currency to be private. For example, a company does not want another company to be able to scan their transactions on the decentralized ledger. In addition to the privacy aspect, being the most crucial property of a cryptocurrency, having zero-fees is an important criterion as well. Especially when making payments

[3] Overview of cryptocurrency market caps: https://coinmarketcap.com
[4] Ethereum: https://www.ethereum.org
[5] ERC-20 Token: https://en.wikipedia.org/wiki/ERC-20

in one country, and not cross-border, people expect these payments to be free of charge. Introducing fees for a new currency would be a step backward in comparison to Fiat money. Last but not least, in a world where it's possible to send messages, pictures or videos all over the world in a matter of seconds, sending money fast will be a standard requirement soon.

1.2.1 Motivation for Privacy

Tixl is not the first cryptocurrency to address the need for private transactions. The number of popular privacy coins currently on the market shows that privacy is an important topic in the area of cryptocurrencies. Among the top 30 cryptocurrencies alone, Monero, Dash and Zcash, for example, focus on private transactions.

The possibilities for the transfer of payments within business environments, as well as private life, are indispensable. The following two examples illustrate this very well.

1.2.1.1 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 the 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. If Bob paid the amount in Tixl, he wouldn't have to pay any fees and Alice would not be able to see Bob's other transactions and vice versa.

1.2.1.2 Example: Point of Sale & E-Commerce

Alice and Bob go to a burger restaurant together, where the restaurant already accepts cryptocurrencies 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 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. If Alice and Bob paid their order in Tixl, there would not be any fees for the payment itself. Also, neither the restaurant nor Alice and Bob would be able to see more transactions of each other. Also, the transaction would settle instantly.

In the case of non-private cryptocurrency such as Bitcoin, the competition can view all transactions going 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 with fiat currencies? 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[6] shows - an open data structure, not having privacy in its core, opens the door for companies being interested in payment data.

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 seven decimal places so that the smallest amount of TXL is 0.0000001.

Realistically the USD equivalent value per TXL will be rather low at the beginning of the project. Therefore, the MTXL unit is also introduced where 1 MTXL (Million TXL) equals 1,000,000 TXL. Exchanges and other websites showing the price of TXL related to other currencies are asked to display the price per MTXL. And as such, the overall supply will be 900,000 MTXL.

1.4 How was the Total Supply Determined?

The total supply of 900,000 MTXL was picked because of psychological reasons which are relevant for the first years of marketing. With 900,000 MTXL being available, 1 MTXL can have the same value as 1 BTC while having approximately only 4 percent of its market cap[7]. Consequently, the value of 1 MTXL will be high compared to Bitcoin or other cryptocurrencies. Limiting the amount of MTXL to this low supply may increase demand, and this may lead to a higher price.

Later on, as soon as TXL is not only seen as an investment opportunity but also used for purchasing goods, exchanges can still display the price of 1 MTXL, but shops can show prices of products in TXL. For example, if Tixl would have a market cap of $90,000,000,000[8], this would mean that 1 TXL equals $0.1[9]. Then if a product in a supermarket cost $1 in Tixl, it would cost 10 TXL. In comparison to other cryptocurrencies, which in most cases have fewer tokens, this is way more applicable than paying fractions of a token for a product.

1.5 How does Tixl Deal with Volatility?

"Volatility is a measure of how much the price of an asset varies over time."[10] The cryptocurrency market is volatile because large trades can result in significant price movements. This, in turn, is since the total market cap of all cryptocurrencies, measured in USD, is much lower than that of less volatile

[6] Benjamin Beck | The Bitcoin Implications of Amazon's New Streaming Data Patent: https://www.allaboutipblog.com/2018/05/the-bitcoin-implications-of-amazons-new-streaming-data-patent/
[7] The exact percentage depends on the circulating supply of both Bitcoin and Tixl.
[8] $90,000,000,000 approximately equals the Bitcoin market cap on April 13, 2019.
[9] If all available TXL would be in circulation. In reality, the circulating supply might be less for a long time.
[10] The Bitcoin Volatility Index: https://bitvol.info/index.html

investments. Consecutively this leads to a chicken-and-egg dilemma because this price instability keeps potential investors away.[11] And it does not only hold potential investors away. It also prevents a cryptocurrency from really being used as a medium of exchange.

The team behind Tixl shares the view of many experts that the market capitalization of cryptocurrencies will rise sharply in the coming years and that volatility will slowly decrease as a result.

For Tixl itself, work is already underway on a concept to reduce volatility by introducing a staking mechanism. Since that is currently under research and development, it will be announced and added to the whitepaper in the future.

[11] Aw Kai Shin: Crypto volatility | The phantom chicken and egg problem: https://medium.com/coinmonks/crypto-volatility-the-phantom-chicken-and-egg-problem-81caf9089cd7

2 Market Overview

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 innovation and putting the conventional 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. Cryptocurrencies do not stop at national borders, and the value is determined worldwide, similar to commodities like gold. 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.

With such rapid development, an essential aspect must not be overlooked: Privacy.

At the beginning of the internet, most people thought they were anonymous because they were behind an IP address. As we know today, this is a pseudo-privacy, and we also have this in Bitcoin with its public addresses. Of course, by only looking at one Bitcoin transaction on the blockchain you will not find out who is behind that transaction. But if you can combine the public ledger with additional data and do some graph analysis combined with the power of machine learning, you will be able to reveal relevant information. Same as privacy was necessary for the internet back in the days; it now becomes important for cryptocurrencies.

Due to the technical implementation of existing solutions, no cryptocurrency has yet been able to fulfill the mandatory requirements of privacy, zero-fee transactions and high transaction speed in a sufficiently collaborative manner. For this reason, Tixl will provide its technical solution, focussing on payments only. The following chapters compare Tixl to different existing cryptocurrencies, attaching particular importance to privacy coins.

2.1 Bitcoin

Bitcoin was the first widely used cryptocurrency. It has thus gained a dominant position and the highest degree of recognition. The myth around the inventor Satoshi Nakamoto was certainly helpful.

Symbol:	BTC
Form of organization:	Community-driven
Launched:	January 3, 2009
Fees:	$0.59 - $0.84[12] *< $0.01 (through Lightning Network)*
Transaction speed:	15 Minutes - 60+ Minutes *almost instant through Lightning Network*
Ledger type:	Blockchain
Cryptosystem for signatures:	Elliptic curve *secp256k1*
Consensus algorithm:	Proof of Work (SHA-256)

Downsides
As a pioneer, Bitcoin could not yet learn from other approaches. Critics point in particular to the elaborate consensus algorithm, which has high energy consumption. In addition, the comparatively high transaction fees and problems in scaling up the transactions per second are also a topic. The fact that mixing services have become more widespread and that there are also recommendations to use a new Bitcoin address for each transaction shows that the lack of privacy is a problem as well.

Ongoing Improvements
By creating the *Lightning Network*, the Bitcoin community invented an off-chain solution tackling some of the Bitcoin scaling issues. It allows much faster, cheaper and even more transactions per second but comes with some trade-offs.[13]

Competition to Tixl
Bitcoin is a direct competitor to Tixl. Since Bitcoin does not support private transactions and also does not have a scaling solution implemented in the Bitcoin core itself, Tixl will be technologically superior. The much more relevant factor in this competition is that Bitcoin has a head start in its prevalence. A lot of good marketing, as well as integrations into payment providers and exchanges, will be required to catch up. However, a co-existence of Bitcoin and Tixl is also possible.

[12] Bitcoin fees: https://bitcoinfees.info/
[13] Jordan Clifford | The Lightning Network; https://medium.com/scalar-capital/the-lightning-network-cf836329626b

2.2 Ethereum

Ethereum is considered a pioneer in using blockchain technology for something other than just a digital currency. One can deploy so-called *smart contracts* on Ethereum. A smart contract is a program on the Ethereum blockchain which can, e.g., represent agreements between different parties as computational code[14]. Besides, Ethereum allows issuing custom assets on their platform, which numerous teams used to conduct ICOs over the past years.

Symbol:	ETH
Form of organization:	Ethereum Foundation (non-profit)
Launched:	July 30, 2015[15]
Fees:	$0.0745[16]
Transaction speed:	~6 Minutes
Ledger type:	Blockchain
Cryptosystem signatures:	Elliptic curve *secp256k1*
Consensus algorithm:	Proof of Work (Ethash) / Proof of Stake deployed on TestNet[17]

Downsides
Ethereum currently has the same weaknesses as Bitcoin.

Ongoing Improvements
As with Bitcoin, the most significant potential for improvement lies in transaction speed and the allowance of private transactions, as well as scalability in general. To defend the leadership position in decentralized apps, a change from Proof of Work to Proof of Stake is being prepared and at least a test network is already available.

Competition to Tixl
Focusing on the execution of smart contracts instead of payments, Ethereum is not a direct competitor to Tixl.

[14] Victor Osetskyi | What Is Smart Contracts Blockchain And Its Use Cases in Business; https://medium.com/existek/what-is-smart-contracts-blockchain-and-its-use-cases-in-business-271a6a23cdda
[15] Ethereum: https://en.wikipedia.org/wiki/Ethereum
[16] Ethereum transaction fees: https://bitinfocharts.com/de/comparison/ethereum-transactionfees.html
[17] Jose Antonio Lanz | The First Ethereum PoS Testnet is Now Live!: https://cryptocrimson.com/the-first-ethereum-pos-testnet-is-now-live/

2.3 Ripple

Ripple has managed to position its software as a payment network for banks bringing many of them onto their platform. Using a type of Federated Byzantine Agreement as their consensus algorithm, Ripple has managed to allow speedy transactions. In addition to its own asset XRP, the Ripple platform also allows issuing and sending other assets.

Symbol:	XRP
Form of organization:	Ripple Labs, Inc.
Launched:	2012
Fees:	$0.0005[18]
Transaction speed:	4 Seconds
Ledger type:	RippleNet[19]
Cryptosystem signatures:	Elliptic curve *secp256k1*
Consensus type:	Federated Byzantine Agreement (FBA)[20]

Downsides
Since everyone can release their token on Ripple's platform and banks can also send assets such as USD directly on RippleNet, the benefit and future of XRP as an asset is questionable. Likewise, there is no privacy protection for transactions beyond that of Bitcoin.

Ongoing Improvements
Ripple is developing on the XRP ledger very actively. Currently, they are focusing more on stability than on larger features. At least that's what is visible to the public.

Competition to Tixl
Since Ripple does not promote XRP as a currency itself but more as a utility token that allows moving value in the network cheaper, it is not a direct competitor to Tixl. However, if Ripple would change their marketing strategy, it would still miss the support for private transactions.

[18] Ripple/XRP transaction fees: https://bitinfocharts.com/de/comparison/xrp-transactionfees.html
[19] Ripple: https://ripple.com/
[20] Shaan Ray | Federated Byzantine Agreement: https://towardsdatascience.com/federated-byzantine-agreement-24ec57bf36e0

2.4 Stellar

Stellar is based on a fork of Ripple. Especially the partnership with IBM has made Stellar popular over the past years. Stellar uses a self-developed variation of the Federated Byzantine Agreement which also supports very fast transactions. Same as with Ripple, it is possible to issue and sent custom assets on the Stellar platform as well as their asset *XLM*.

Symbol:	XLM
Form of organization:	Stellar Development Foundation (non-profit)
Launched:	July 31, 2014
Fees:	0.00001 XLM[21]
Transaction speed:	3-5 Seconds[22]
Ledger type:	Stellar Network
Cryptosystem signatures:	Elliptic curve *ed25519*
Consensus algorithm:	Federated Byzantine Agreement (FBA)

Downsides
Stellar currently has the same weaknesses regarding private transactions as Ripple.

Ongoing Improvements
In 2019 the Stellar foundation plans to improve the decentralization of the Stellar network while preserving performance.[23]

Competition to Tixl
Stellar is quite comparable to Ripple when looking at the way it competes to Tixl.

[21] BlockEQ | Transaction Fees on Stellar: https://medium.com/@blockeq/transaction-fees-on-stellar-3d5e442fc00a
[22] What is Stellar Blockchain?: https://blockgeeks.com/guides/what-is-stellar-blockchain/
[23] Stellar Roadmap: https://www.stellar.org/roadmap

2.5 Monero

Monero is considered the father of the privacy coins. To obfuscate the origins, amounts, and destinations of all transactions Monero uses *ring signatures*, *ring confidential transactions*, and *stealth addresses*. Thus, transactions on the Monero blockchain don't link to a particular user or real-world identity.[24]

Symbol:	XMR
Form of organization:	Community-driven
Launched:	2014
Fees:	$0.0197[25]
Transaction speed:	~20 Minutes[26]
Ledger type:	Blockchain
Cryptosystem signatures:	Elliptic curve *ed25519*[27]
Consensus algorithm:	Proof of Work (CryptoNote)

Downsides
As a fork from Bitcoin, Monero also suffers from the same problems regarding transaction speed, scalability, and the rather high fees. In addition, it is questionable how effective the ring signatures protect the sender when large amounts of data are available for analysis.

Ongoing Improvements
According to the Monero roadmap, future work will focus on improving transaction speed and scalability by second layer solutions.[28]

Competition to Tixl
Same as Tixl, Monero targets private payments, so it is a serious competitor. From all privacy coins, it currently has the highest market cap. Nevertheless, Monero's scaling problems open the door for Tixl to compete with it.

[24] https://www.getmonero.org/
[25] Monero Transaction Fees: https://bitinfocharts.com/de/comparison/monero-transactionfees.html
[26] Monero Transaction Speed: https://www.monero.how/how-long-do-monero-transactions-take
[27] Edwards25519 Elliptic Curve: https://monerodocs.org/cryptography/asymmetric/edwards25519/
[28] Monero Roadmap: https://www.getmonero.org/resources/roadmap/

2.6 Zcash

Like Monero, ZCash is a fork from Bitcoin but uses a different Proof of Work algorithm called *Equihash*. Unlike Monero, the Zcash Ledger distinguishes between *transparent* and *shielded* addresses. So Zcash allows both private as well as public transactions on one ledger. To achieve privacy with shielded addresses, Zcash uses so-called zero-knowledge proofs, specifically *zk-SNARKs*. Zero-knowledge proofs are widely considered the most bleeding edge cryptography available.[29]

Further positive development at Zcash is that the New York State Department of Financial Services approved trading the privacy-protecting cryptocurrency.[30]

Symbol:	ZEC
Form of organization:	Zcash Foundation (non-profit)
Launched:	October 28, 2016
Fees:	$0.00000432[31]
Transaction speed:	~15 Minutes
Ledger type:	Blockchain
Cryptosystem signatures:	Elliptic curve *BLS12-381*
Cryptosystem encryption:	Elliptic curve *BLS12-381*[32]
Consensus algorithm:	Proof of Work (Equihash)

Downsides
With zk-SNARKs, Zcash currently offers the probably strongest privacy on a publicly accessible ledger. Up to now, it was very time-consuming to generate the corresponding proofs before sending a transaction. In the last few months, however, considerable speed improvements have been achieved. Nevertheless, scalability will remain a major pain point for Zcash in the near future.

It is also noticeable that only a tiny proportion of transactions make use of the privacy feature. One of the reasons for this is that many wallets only support transparent addresses yet.

Furthermore, earlier this year, an Equihash-compatible ASIC miner was announced by Bitmain, which opens up Zcash's future to miner centralization similar to Bitcoin.[33]

Ongoing Improvements
According to what they say on meetups and conferences, the Zcash team will concentrate on scalability over the next years. Zcash's roadmap also doesn't point out other features.[34]

Competition to Tixl
Zcash is a direct competitor to Tixl and has the best privacy concept from all other cryptocurrencies. It has a lower market cap than Monero but a higher daily transaction volume. For Zcash the same opportunities apply as for Monero, the advantages in scalability make Tixl a severe competitor.

---

[29] Griffin Knight | Monero vs. Zcash and the Race to Anonymity: https://medium.com/coinmonks/monero-vs-zcash-and-the-race-to-anonymity-4322b0a9bd90
[30] David Benger | Zcash & The New York State: https://coincenter.org/link/the-new-york-state-department-of-financial-services-just-approved-the-trading-of-privacy-protecting-cryptocurrency
[31] Zcash Transaction Fees: https://bitinfocharts.com/de/comparison/zcash-transactionfees.html
[32] zk-SNARK Elliptic Curve Construction: https://z.cash/blog/new-snark-curve/
[33] Examples of pivacy coins: https://blog.liquid.com/examples-of-privacy-coins-monero-zcash-dash
[34] Zcash Roadmap: https://z.cash/support/schedule

2.7 Dash

Like Zcash, Dash offers both transparent and private transactions. Private transaction capability is made possible via the implementation of *CoinJoin*. Dash calls this *PrivateSend*. CoinJoin is a trustless tool that combines or mixes multiple transactions into a single transaction to obscure the exact transaction flow of each transaction.[35]

Symbol:	DASH
Form of organization:	Dash Core Group, Inc.
Launched:	January 18, 2014
Fees:	$0.0084[36]
Transaction speed:	~15 Minutes[37]
Ledger type:	Blockchain
Cryptosystem signatures:	Elliptic curve *secp256k1*[38]
Consensus algorithm:	Proof of Work (X11)

Downsides
Dash claims to be decentralized, but the implementation of CoinJoin is not very decentralized at all. PrivateSend transactions on the Dash network are processed by master nodes. If a single entity can control or spy on a portion of Dash's master nodes, it's entirely possible to reverse engineer PrivateSend transactions to reveal origin and destination details.

Like Zcash, Dash has struggled with the adoption of its privacy features. In Dash's case, the issue mainly revolves around liquidity. Since PrivateSend is a CoinJoin implementation, it requires liquidity and demand to mix effectively and privately. Dash's master node and mixing liquidity provider model puts privacy features on a second tier that is more prone to centralization.[39]

Ongoing Improvements
According to Dash's roadmap[40], the team will focus on improving its wallet software in 2019. Dash plans to implement features like providing a username or connecting with contacts. These indicate that they are targeting Paypal-like features.

Competition to Tixl
Even though Dash does not compete with Zcash's enhanced privacy protection, the team behind Dash is very experienced in doing marketing for its currency. Being within the top 20 cryptocurrencies in terms of market cap, Dash is also a severe competitor to Tixl.

[35] Examples of pivacy coins: https://blog.liquid.com/examples-of-privacy-coins-monero-zcash-dash
[36] Dash Transaction Fees: https://bitinfocharts.com/de/comparison/dash-transactionfees.html
[37] Mark Schwarz | Transaction Speeds: https://www.abitgreedy.com/transaction-speed/
[38] Dash Public Key: https://github.com/dashevo/dashcore-lib/blob/master/docs/publickey.md
[39] LIQUID | Examples of privacy coins: Monero, ZCash, DASH: https://blog.liquid.com/examples-of-privacy-coins-monero-zcash-dash
[40] Dash Roadmap: https://www.dash.org/roadmap/

2.8 Grin

Grin's stated goal is to produce a simple and easy to maintain implementation of the *Mimblewimble* protocol. "MimbleWimble, or MW in short, is an approach that was proposed [...] to improve the privacy features of Bitcoin. Some people liked the idea of MW and saw it as a simple and reasonably effective way to achieve transaction privacy. However, because the MW approach required significant changes to Bitcoin, it was largely dismissed by the Bitcoin community. Since then, MW did not see significant discussion or development until it came to the front page of crypto with Grin."[41] Grin is designed to be inflationary, and the potential supply of Grin is infinite.[42]

Symbol:	GRIN
Form of organization:	Community-driven[43]
Launched:	January 15, 2019
Fees:	> $0[44]
Transaction speed:	> 1 Minute[45]
Ledger type:	Blockchain
Cryptosystem signatures:	Elliptic curve *secp256k1*[46]
Cryptosystem encryption:	Elliptic curve *secp256k1*
Consensus algorithm:	Proof of Work (Cuckoo Cycle)

Downsides

"When MW transactions are published to the unconfirmed transaction (TX) pool, the TX inputs and outputs are still visible. Miners are required to create the transaction blocks in a way that allows transaction cut-through to hide some of this information. The confirmed block will have a smaller number of inputs and outputs mixed together in a way that makes it more difficult to recognize the sides of a specific transaction. However, it is possible and probably easy for anyone to keep recording all the transactions from the unconfirmed transaction pool. This data could be used to build detailed transaction graphs of the network. [...] In fact, it can be very profitable to have data that most people think is impossible to have. The privacy guarantee of MimbleWimble, in this case, is equivalent to using Bitcoin with generating a new address for each new transaction (with the added advantage of hiding the TX amount)."[47]

Ongoing Improvements

At MimbleWimble's current stage of development, the privacy guarantees are lower than Monero and Zcash. That may change in the future. It may be possible with additional developments to the

[41] Mohamed Fouda | MimbleWimble: The Good and the Bad: https://www.tokendaily.co/blog/mimblewimble-the-good-and-the-bad
[42] Christopher Williams | GRIN & BEAM: How Revolutionary are the New MimbleWimble Privacy Coins?: https://dapplife.com/grin-beam-how-revolutionary-are-the-new-mimblewimble-privacy-coins/
[43] Grin vs. BEAM, a Comparison: https://tlu.tarilabs.com/protocols/grin-beam-comparison/MainReport.html
[44] Grin Economic Policy: Fees and Mining Reward: https://github.com/mimblewimble/grin/wiki/fees-mining
[45] TM Lee | Grin: Frequently Asked Questions: https://www.coingecko.com/buzz/grin-frequently-asked-questions
[46] Grin forum discussion: https://www.grin-forum.org/t/schnorr-signatures-in-grin-information/730
[47] Mohamed Fouda | MimbleWimble: The Good and the Bad: https://www.tokendaily.co/blog/mimblewimble-the-good-and-the-bad

MimbleWimble protocol to reach a privacy level comparable to Monero. However, it may not be possible to achieve the privacy guarantees of Zcash shielded transactions without further encryption.[48]

Competition to Tixl
Although Grin cannot compete with the privacy of Zcash, Grin benefits from the interest in implementations of the MimbleWimble protocol. Grin is still at the very beginning of its distribution and does not have much of a lead over Tixl. MimbleWimble's attention may help Grin to become a competitor for Tixl in the long run.

2.9 Beam

Beam is also an implementation of the MimbleWimble protocol. It supports both confidential and non-confidential transactions. Beam is using a deflationary model with a periodic halving of their mining reward and a maximum supply of BEAM of ~262 million coins. The team behind Beam has set themselves the goal to extend the feature set of Mimblewimble in several ways. That includes, for example, an implementation of an auditable wallet and a feature that allows asynchronous negotiation of transactions.[49]

Symbol:	BEAM
Form of organization:	Beam Development Ltd.[50]
Launched:	January 3, 2019
Fees:	> $0
Transaction speed:	> 1 Minute[51]
Ledger type:	Blockchain
Cryptosystem signatures:	Elliptic curve *secp256k1*[52]
Cryptosystem encryption:	Elliptic curve *secp256k1*
Consensus algorithm:	Proof of Work (modified Equihash)[53]

Downsides
Beam currently has the same weaknesses as Grin.

Ongoing Improvements
According to the Beam roadmap, future work will focus on different topics. These include scalability, wallets for various platforms, payment platform integrations and an alternative consensus algorithm.[54]

Competition to Tixl
Although Beam, like Grin, can't compete with Zcash's privacy, Beam could become a serious competitor for Tixl in the long run with the extensive feature list on the roadmap.

---

[48] Mimblewimble: the good and the bad: https://thebitcoin.pub/t/mimblewimble-the-good-and-the-bad/49971
[49] Grin vs. BEAM, a Comparison: https://tlu.tarilabs.com/protocols/grin-beam-comparison/MainReport.html
[50] Beam FAQ: https://www.beam.mw/faq/what-is-beam-model-of-governance
[51] Beam FAQ: https://www.beam.mw/faq/what-is-the-block-time-and-block-size
[52] Beampedia: https://www.beam.mw/beampedia-item/elliptic-curve-cryptography
[53] Rachel Rose O'Leary | Grin and Beam: A Tale of Two Coins Being Built on Mimblewimble: https://www.coindesk.com/grin-and-beam-a-tale-of-two-coins-being-built-on-mimblewimble
[54] Beam 2019 Roadmap: https://medium.com/beam-mw/mimblewimble-beam-roadmap-2019-b2c7f38fc106

2.10 Nano

Using its block-lattice structure, Nano wants to succeed where Bitcoin has fallen short. The cryptocurrency promises to deliver zero-fee transactions in real time without the same work-intensive overhead and energy consumption as Bitcoin.

The block-lattice infrastructure operates as a blockchain but with a few key differences. To start, each account on Nano's protocol has its blockchain, called an account-chain. Only an account-chain's user can modify their individual chain, and this allows each account-chain to be updated asynchronously of the rest of the block-lattice network.

By implementing a dual-transaction mechanism, it's up to both the receiver and sender of funds to verify a transaction. That eliminates the need for miners and paves the way for instant and zero-fee transactions.[55]

Symbol:	NANO
Form of organization:	Nano Foundation (non-profit) and NanoLabs Inc.
Launched:	October 7, 2015
Fees:	$0
Transaction speed:	~15 Seconds[56]
Ledger type:	Block-lattice (DAG)
Cryptosystem signatures:	Elliptic curve *ed25519*
Consensus type:	Delegated Proof of Stake

Downsides
Over the past, a nano transaction was possible in less than 3 seconds because only conflicting transactions were voted on by the consensus algorithm. But in exchange for finality, which was not present in the beginning, the transaction time has increased significantly. On Reddit users report that transactions sometimes take even more than 20 seconds. As a result, Nano has also lost some of the charms of the super-fast transactions.

Nano ignores this lack of private transactions, and it is questionable whether Nano can implement such a feature without further significant changes.

Ongoing Improvements
According to the Nano roadmap, future work will focus on improving transaction speed and decentralization.[57]

Competition to Tixl
Nano has a comparable feature set to Tixl. However, the privacy aspect is currently not considered, and the Nano team does not seem to work on private transactions. In the long term, Nano is therefore not positioned as a direct competitor.

[55] Colin Harper | What Is Nano?: https://coincentral.com/nano-beginners-guide/
[56] Reddit discussion: https://www.reddit.com/r/nanocurrency/comments/ald1et/nano_is_not_instant_at_least_not_literally
[57] Nano Roadmap: https://developers.nano.org/roadmap/

2.11 Tixl

Tixl uses the advantage of a green field implementation and combines the best components of the existing currencies in one. Like Nano, Tixl uses a directed acyclic graph as its data structure. Same as for Nano, this supports instant transactions. To have a decentralized system that votes for conflicting transactions, Tixl uses the Stellar Consensus Protocol (SCP) which which even solves conflicts quickly. Last but not least, Tixl makes usage of quantum secure cryptography, which is not used by any other competitor.

Symbol:	TXL
Form of organization:	Tixl gGmbH (non-profit)
Launched:	not yet available
Fees:	$0
Transaction speed:	~1-5 Seconds (expected)
Ledger type:	Block-lattice (DAG)
Cryptosystem signatures:	XMSS (expected)
Cryptosystem encryption:	NTRU (expected)
Consensus type:	Federated Byzantine Agreement (FBA)

Downsides
While the time to develop Tixl now is very advantageous in terms of being able to use the different technical concepts and experiences of the other coins, there are also disadvantages. The existing coins, of course, have a lead in terms of awareness, exchange listings, volume and especially the supporting community. While the other currencies are already live, Tixl is still in development.

2.12 Final Thoughts

We've seen lots of technological progress in the field of cryptocurrencies over the last years. For example, the quantum secure cryptosystem NTRU was released out of patent and developers all over the world can now use it. Also, alternative data structures and consensus algorithms have proven themselves. That means there is not only that one simple blockchain anymore. It's also no secret that there are better methods in a decentralized system to find out if a transaction is valid then the rather slow and power consuming Proof of Work algorithm of Bitcoin.

Developing Tixl a few years ago would not have been possible as that would have required extensive research in all of the crucial base technologies - cryptography, data structure and finding consensus.

3 Fundraising

Tixl makes use of a token sale for fundraising. ICO[58] is the abbreviation for Initial Coin Offering. ICOs are an alternative to traditional fundraising methods and have proven themselves in recent years for projects that use blockchain or focus on decentralization. If an ICO is performed directly on an Exchange, it is referred to as an Initial Exchange Offering (IEO).

Legal disclaimer: For all information about the fundraising, please also refer to the general terms and conditions.[59]

3.1 Why should an Token Sale 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 must be commissioned.

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. However, 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 USD, EUR or other Fiat currencies.

3.2 How is it Possible to Distribute Tixl Tokens during the Token Sale Although Tixl is still being Developed?

During the token sale, no real TXL but instead Tixl tokens, named *TXLT*, on an existing platform will be sold. More precisely, they are launched as *MTXLT* (stands for one million TXLT) on the Stellar platform [60]. To receive (M)TXLT a Stellar wallet is required.

After completion of the technical development of TXL, the Tixl token holders are offered to swap their Tixl tokens (TXLT) for TXL at a ratio of 1 to 1. In other words, Tixl Token holders can swap their Stellar based MTXLT for TXL at a ratio of 1 to 1,000,000 (one million). This method is called *token swap* and was also practiced for example by *EOS*.

[58] Initial Coin Offerings (ICOs) explained: https://www.investopedia.com/terms/i/initial-coin-offering-ico.asp
[59] Tixl General Terms and Conditions: https://tixl.me/legal/general-terms-and-conditions
[60] Stellar Platform: https://www.stellar.org/

3.3 Token Swap

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[61]. 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 the Tixl 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.[62]

3.4 How many TXLT are Sold for Fundraising and what Happens to the Rest?

Diagram 1 shows an overview of the TXLT distribution. It is noticeable that by far the most substantial part is intended for the token sale. The following list describes in detail how the other TXLT are planned to be used.

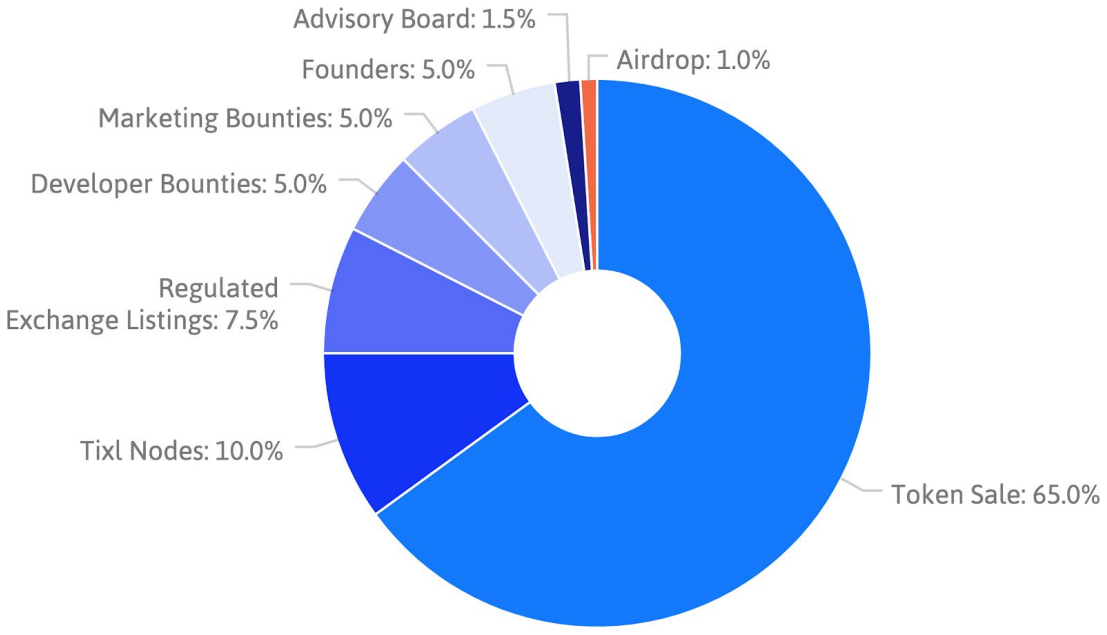

Diagram 1: TXLT distribution

Token Sale (65%): By far the most substantial amount of TXLT is offered during the token sale.

Tixl Nodes (10%): The hosting of Tixl is associated with computing power that needs to be provided by someone. Chapter 5.4.4 discusses how TXL can be used as an incentive.

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

Regulated Exchange Listings (7.5%): Exchange listings are crucial to the distribution of a cryptocurrency. With this additional provision, exchanges could be offered TXL to become listed.

Developer Bounties (5%): Tixl will release 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, performance improvements, 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 TXL(T). For instance, it is considered to provide an amount of TXL to payment providers integrating and promoting payments with TXL. Another option for a marketing bounty would be to let YouTubers explain the Tixl concept and get TXL(T) in return.

Founders (5%): The founders will finance the initial stage of the project and the preparations for the fundraising. These include designs (logo, CI, documents), trademark application and legal advice being the most significant 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%): Tixl will have a board of advisors. Depending on the situation, there should be a small reward in the form of TXL(T) for those advisors.

Airdrop (1%): Some TXLT are given away for free (see chapter 3.7).

3.5 At what Price Levels will TXLT be Offered?

The Tixl fundraising will be conducted in five phases starting in Q2 2019. Table 1 shows the periods, amounts of tokens for sale and the token prices in USD per MTXLT. Phase 3 in Q4 2019 will be conducted as an IEO with a $9,000,000 hard-cap. The previous phases are accordingly referred to as Pre-IEO and have lower price levels.

The strategy for the following phases of the fundraising depends on the success of the previous phases. It is also considered to target larger investors like VCs or family offices in phases 4 and 5. To avoid that tokens sold in these phases will be traded on exchanges immediately afterward, purchases from these phases will have minimum holding periods. Once a strategy was defined, announcements of phases 4 and 5 will be published on the Tixl website.

Phase	Period (Quarter / Year)	MTXLT for Sale	Price per MTXLT
1	Q2 / 2019	22,500	$20
2	Q3 / 2019	45,000	$50
3	Q4 / 2019	90,000	$100
4	Q1 / 2020	135,000	to be announced
5	Q2 / 2020	292,500	to be announced
	Total	**585,000**	

Table 1: Tixl Fundraising Phases

3.6 What Happens to TXLT Not Sold in the Token Sale?

TXLT not sold in the token sale 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 the termination of the token sale may one of these packages be offered monthly for public or private sale. If a package is not entirely sold, it will be automatically appended to the 60-month escrow again. The way this escrow behaves is pretty similar to how Ripple conducts its sales.[63]

3.7 Airdrop

To boost marketing before and during the fundraising a TXLT airdrop started on March 18, 2019 at 12:00 pm GMT. During this airdrop, 1% of the overall TXLT supply, or in numbers 9,000 MTXLT 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 MTXLT 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 3.6).

Not before January 01, 2020, airdropped TXLT will be sent out on the Stellar platform. That is to avoid airdropped TXLT being sold for the first phases of the fundraising. An airdrop participant must store their public Stellar address on the account page until December 31, 2019 at 12:00 pm GMT. It's required that the corresponding Stellar account is activated and contains enough balance to establish a trustline with the Tixl Stellar issuer address. In case a participant does not provide a Stellar address or does not establish the necessary trustline, 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's 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.[64]

3.8 Airdrop Referral Program

There will be a referral program only for the airdrop. 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.

If a referred participant refers another participant the first referrer will also get some extra TXLT. An example better explains this. Participant A refers participant B, participant B refers participants C and D. Now the credits would be:

$$A = 100\ TXLT + 100\ TXLT\ (ref\ B) + 20\ TXLT\ (B\ ref\ C) + 20\ TXLT\ (B\ ref\ D) = 240\ TXLT$$
$$B = 100\ TXLT + 100\ TXLT\ (ref\ C) + 100\ TXLT\ (ref\ D) = 300\ TXLT$$

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

$C = 100\ TXLT$
$D = 100\ TXLT$

As the example calculation shows, participant A will get 20% from 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.

$A = 100\ TXLT + 100\ TXLT\ (ref\ B) + 20\ TXLT\ (B\ ref\ C) + 20\ TXLT\ (B\ ref\ D) + 10\ TXLT\ (C\ ref\ E) = 250\ TXLT$
$B = 100\ TXLT + 100\ TXLT\ (ref\ C) + 100\ TXLT\ (ref\ D) + 20\ TXLT\ (C\ ref\ E) = 320\ TXLT$
$C = 100\ TXLT + 100\ TXLT\ (ref\ E)$
$D = 100\ TXLT$
$E = 100\ TXLT$

The referral bonus will only be credited in case the referred airdrop participant follows the steps from chapter 3.7 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 3.7.

3.9 Fund Utilization

This financial planning shall in particular address the use of the capital collected from the fundraising. Fundraising phases 1 and 2, as well as everything beyond them, are considered separately for this purpose. The following graphs describe how the money from the collected phase(s) will be used. However, the expenses for this do not arise directly in the same phase

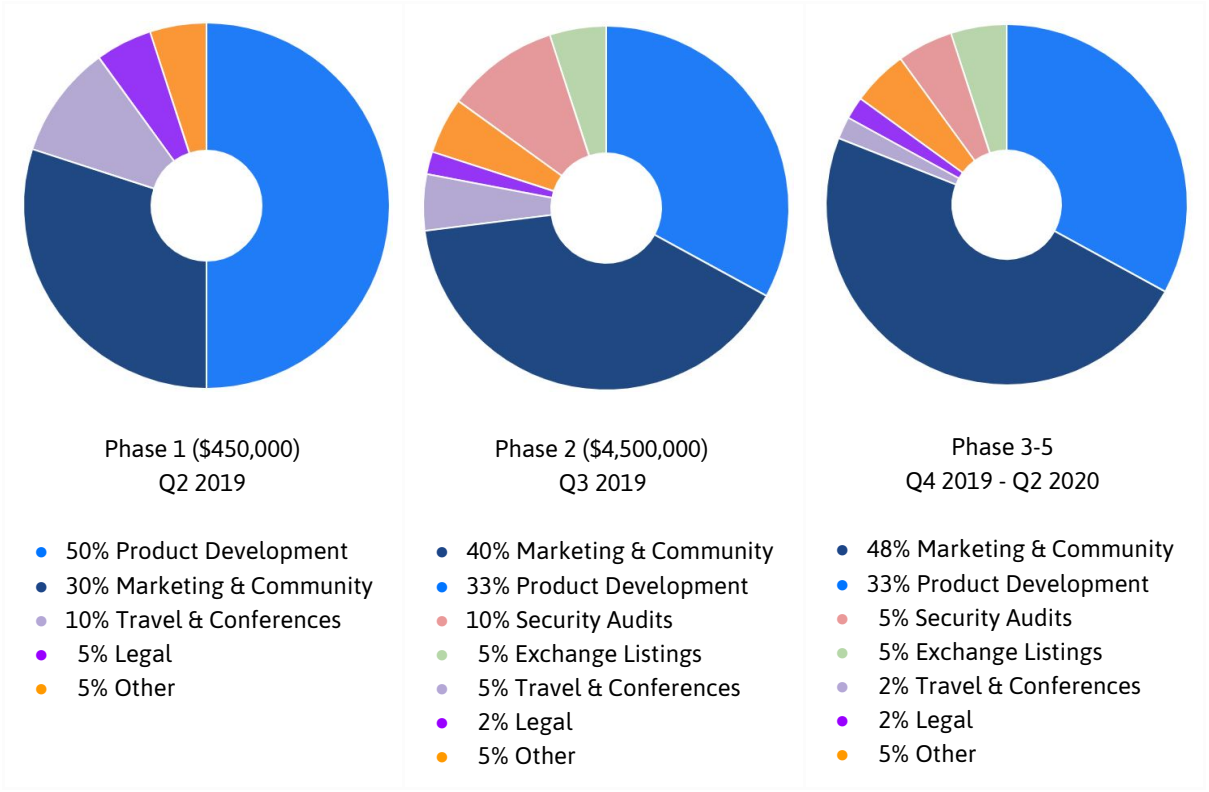

Diagram 2: Fund Utilization

The planned expenses have been categorized into different areas:

Product Development
Product Development bundles all expenses related to the software development of Tixl. In particular, these are mostly personnel costs for software development. Besides, these expenses also include costs for required hardware, conception, and operation of a test network.

Marketing & Community
At least as important as software development is the marketing of Tixl and the maintenance and communication with the community. The planned budget is correspondingly high to ensure that Tixl will be successful in the long term. From phase 2 onwards, the budget is even larger than for the product development itself.

Travel & Conferences
Especially in the early days, it's important to present Tixl at appropriate conferences and other events. Travel costs are incurred, and sometimes speaker slots have to be purchased. Since the purchase of speaker time probably decreases with increasing awareness, and organizers might subsidize travel costs entirely, the share for travel and conferences is decreasing in the later phases.

Legal
Legal costs have been incurred in preparing for the fundraising. We expect that further expenses for legal advice will also be incurred later in the project. Examples of legal costs include reviewing updated versions of the whitepaper and filing patents if necessary. Also, there are ongoing costs for accounting and tax consulting.

Security Audits
The security of the system is crucial. Therefore different forms of security audits and hacker attacks on a test network are planned in different phases.

Exchange Listings
To ensure good availability for as many people as possible, listing on regulated exchanges is unavoidable. Good availability also has a positive influence on Tixl's price development. Accordingly, budget planning also takes that into account.

Other
That includes other expenses such as office rent, KYC provider fees or software tools. At the same time, it serves as a small buffer for unforeseen costs.

3.10 Investment Potential

Legal disclaimer: There is no guarantee that MTXLT or later MTXL will increase in value. At this point, we would like to point out the risks in chapter 7.

Table 2 shows various ways in which an investment in Tixl could develop. Each row represents a possible case and the price development in USD. The column *Price per MTXLT* refers to the purchase price of tokens during the token sale. Multiplied by the *Amount of MTXLT Purchased* this results in the *Total Purchased Value*. To determine the value of the column *Value at One Billion $ Market Cap*, a definition of the derivation for the market cap is required:

$$MTXLT\ Market\ Cap\ (USD)\ =\ Circulating\ Supply\ *\ Price\ per\ MTXLT\ (USD)$$ [65]

For the investment cases in Table 2, a circulating supply of 515,250 MTXLT is assumed, representing 57.25% of the total supply (900,000 MTXLT). This value can be derived as follows:

$$\begin{aligned}
&9,000\ MTXLT\ distributed\ in\ airdrop\\
&+45,000\ MTXLT\ for\ founders\\
&+371,250\ MTXLT\ sold\\
&\quad 22,500\ MTXLT\ (Phase\ 1)\\
&\quad 45,000\ MTXLT\ (Phase\ 2)\\
&\quad 90,000\ MTXLT\ (Phase\ 3)\\
&\quad 213,750\ MTXLT\ (Phase\ 4\ and\ 5\ if\ only\ 50\%\ sold)\\
&+90,000\ MTXLT\ for\ marketing,\ exchange\ listings,\ etc.\\
&=515,520\ MTXLT
\end{aligned}$$

The investment cases in Table 2 refer to a market capitalization of $1,000,000,000. That corresponds, for example, to the current market capitalization of Monero[66]. If the price per MTXLT in USD with a market cap of $1,000,000,000 is to be determined, the following calculation applies:

$$Price\ per\ MTXLT\ (USD)\ =\ \frac{\$1,000,000,000}{515{,}520\ MTXLT}\ =\ \$1,939.79$$

This price can now be multiplied by the *Amount of MTXLT Purchased*, resulting in the *Value at One Billion $ Market Cap*. The *Return on Invest* (ROI) is then calculated by:

$$ROI\ =\ \frac{Value\ at\ \$1{,}000{,}000{,}000\ Market\ Cap}{Total\ Purchased\ Value}$$

Of course, the goal is to achieve a higher market capitalization with Tixl. Accordingly, the figures in Table 2 retain an upward room for maneuver.

Case No.	Price per MTXLT	Amount of MTXLT Purchased	Total Purchased Value	Value at One Billion $ Market Cap	ROI
1		10	$200	$19,398	
2	$20	100	$2,000	$193,979	~97x
3		1000	$20,000	$1,939,789	
4		5	$500	$9,699	
5	$100	50	$5,000	$96,989	~19x
6		500	$50,000	$969,894	

Table 2: Investment Potential

[65] The *circulating supply* is the quantity of a currency in circulation.
[66] The market cap of Monero equals $1.039.952.675 as of April 30, 2019.

4 Organizational Form

4.1 Team

The Tixl team consists of seven core members. Since Tixl is a company of the elbstack GmbH, the Tixl gGmbH can additionally use the services of the elbstack GmbH to a certain extent. In the past, different team members of elbstack helped Tixl with feedback, code reviews or design improvements. The following is a brief overview of the individual team members.

Christian Eichinger
Managing Director & Founder[67]

- M.Sc. Software Engineering Leadership
- Founded elbstack in 2015 and scaled the company up to 20 employees in 2019 being profitable all the time
- Expert in translating mathematically defined cryptography to source code

Roles at Tixl
- Business Development & Finance
- Implementation of the Tixl ledger core cryptography

Sebastian Gronewold
Managing Director & Founder

- M.Sc. Software Engineering Leadership
- Founded elbstack in 2015 and scaled the company up to 20 employees in 2019 being profitable all the time
- Started to study alternative consensus algorithms early in 2017 when Proof of Work was still state of the art

Roles at Tixl
- Business Development & Marketing
- Implementation of the Tixl consensus algorithm and API gateway

Christopher Obereder
Chief Marketing Officer (CMO)

- Marketing at Harvard Ventures (Harvard University)
- 27-year-old serial entrepreneur, Forbes 30 under 30 member and one of leading growth hackers worldwide
- CMO of the mobile portfolio management app Coin Stats with over 600,000 active portfolios tracked worldwide

Roles at Tixl
- Marketing
- Fundraising
- Public Relations

Mike Lohmann
Technology Consultant

- Founded elbstack in 2015 and scaled the company up to 20 employees in 2019 being profitable all the time
- Has deep knowledge and years of experience in setting up complex software architectures that can scale up to millions of users
- Helped lots of companies stress testing their environments before starting large marketing campaigns

Roles at Tixl
- Consultancy regarding technological decisions
- Review of the software architecture

[67] In Germany “CEO” is not a legal term and a company can have multiple CEOs

Bernd Strehl
Software Engineer

- M.Sc. Information Systems
- Joined elbstack in 2018
- Outstanding knowledge in implementing complex algorithms for different use cases
- Creator of serverless-benchmark.com
- Strong experience in programming smart contracts based on Ethereum

Roles at Tixl
- Implementation of the Tixl consensus algorithm

Vihren Stoev
Cryptographer

- B.Sc. Mathematics
- Expert in several cryptosystems
- Came in touch with quantum secure cryptography over 10 years ago

Roles at Tixl
- Implementing the cryptosystems for signatures and the encryption of transaction amounts

Lennart Brandt
UX and Digital Product Designer

- B.Sc. Information Systems
- Joined elbstack in 2016
- Has built fancy UIs for several companies across Germany
- Creator of the intermittent fasting app *Chew*

Roles at Tixl
- UI and UX Design
- Frontend Development

4.2 Business Model

Since Tixl carries out transactions 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 token sale and later by potentially selling 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 installments. Also after the vesting period, there will be a maximum amount of TXL that can be sold per month.

4.3 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. To achieve this, Tixl is founded as a German non-profit limited liability company - the *Tixl gGmbH*. A transfer to a foundation at a suitable time is conceivable but not mandatory.

4.4 Trademark and Patent Rights

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

People frequently quote centralization as a criticism against patent applications. For instance, at some point, the community might advocate an opinion on the development of Tixl, which diverges significantly from the idea 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 the Tixl network.

5 Technical Solution

The technical solution is one of the decisive factors for superiority over existing cryptocurrencies. A combination of different aspects puts Tixl in this position. The most important parts are Tixl's data structure, the applied cryptosystem, a guarantee of real privacy and its chosen consensus algorithm.

5.1 Data Structure

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

5.1.1 Which Data Structure does Tixl use to Persist Transactions?

The Tixl ledger is a special implementation of a *Directed Acyclic Graph* (DAG)[68]. The implementation of Tixl is similar to the *block-lattice*[69] architecture of Nano. A special feature here is that every user has their blockchain and only the owner of a 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 number of transaction partners.

5.1.2 Block Structure

Data in a block on the Tixl Ledger can be divided into four groups:

1	**Metadata (unencrypted)**	• Reference to the previous block • Block type • Further public information
2	**Data for the receiver (encrypted)**	• Destination address • Transaction amount • Description
3	**Data for the sender (encrypted)**	• Transaction amount • New account balance on stealth-chain • Description
4	**Data for validation (unencrypted)**	• Block signature • Commitments for the zero-knowledge proofs • Micro Proof of Work for spam protection

Figure 1: Block Structure

Metadata (unencrypted)
The metadata contains various data relevant to the block. These include a reference to the previous block and the block type.

Data for the receiver (encrypted)
There is information that the recipient should receive without anyone else on the network being able to read it. That includes the amount of the transaction and an optional description.

[68] Sherman Lee | Explaining Directed Acyclic Graph (DAG), The Real Blockchain 3.0: https://www.forbes.com/sites/shermanlee/2018/01/22/explaining-directed-acylic-graph-dag-the-real-blockchain-3-0/
[69] Block Lattice: https://github.com/nanocurrency/raiblocks/wiki/Block-lattice

Data for the sender (encrypted)
The sender would also like to be able to view the amount sent afterward. Therefore the sender encrypts specific data for himself. In addition to the amount, this also affects the balance on the stealth-chain. In case the block is a receive block, this part is omitted.

Data for validation (unencrypted)
To verify transactions by consensus, certain data is required. In this part of the block, the block signature, commitments for the zero-knowledge proofs and the micro Proof of Work for spam protection are stored.

Encrypting a small amount of data both for the sender and for the recipient produces duplicate data. This overhead will be accepted in favor of privacy.

5.1.3 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 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[70]. Due to the cryptographic requirements, Tixl transactions are expected to consume slightly more storage space.

5.1.4 Scalability

Tixl's data structure is a good prerequisite for scalability. In terms of the required storage space for the full ledger, Tixl pretty much scales like Bitcoin or other cryptocurrencies except that it has the encryption overhead. Regarding the transaction speed, the data structure itself supports instant transactions because only senders and receivers are involved instead of the whole network.

5.1.4.1 Is a Tixl Transaction Really Instant?

Essentially, the Tixl data structure allows instant transactions. Senders and receivers can write transactions on their blockchains without having to wait for other transactions on the network. Nano also advertises these *Instant Transactions*. However, it should be noted that a recipient must be online if a transaction is to be written to the recipient's blockchain immediately after submission.

In practice, however, more aspects must be considered. As a Tixl receiver, one cannot always 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 validation takes time because the decentralized entity must decide on a consensus relevant to the validity of a transaction. Even if this executes within a few seconds, Tixl envisions additional mechanisms of trust to further accelerate transactions (to be announced in the future).

5.2 Which Cryptosystem does Tixl use?

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

[70] Nano Whitepaper: https://nano.org/en/whitepaper

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 make practical progress on them finally. 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 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.

5.2.1 Quantum Security in Tixl

Tixl uses cryptography in different parts of its software. Of course, signing transactions itself and encrypting transaction details requires cryptography. On the other hand, the consensus algorithm uses signing and encryption methods as well, for example, to securely communicate with other nodes.

Since the Tixl prototype is currently being developed, a final decision for the utilized cryptosystem cannot be made. However, *XMSS* is considered for the signature part and, for the encryption part, *NTRU* seems to be a good fit. The Tixl prototype already uses both of them.

5.2.2 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, people praised the new cryptosystem 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, NTRU drew new attention, and the different attacks were studied much better. 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.[71]

5.2.3 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. That makes XMSS also forward-secure which means that even if a secret key is compromised, all previous signatures remain valid and are not compromised.

5.3 Private Transactions

Tixl achieves private transactions 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 (*account-chain*) of a user but instead to unclassifiable blockchains (*stealth-chains*) 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. Tixl achieves that by sending TXL directly from stealth-chains that a new recipient cannot relate with other TXL owners.

The section about confidential transactions explains how it is possible for the amount of a transaction, as well as the account balances, 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.

5.3.1 Account-chain

The account-chain represents the user's main account. It is used to store encrypted references to the user's stealth-chains.

5.3.2 Stealth-chain

A stealth-chain is a separate blockchain that works much like a Monero stealth address[72]. For each sender/receiver combination, the first transaction generates a new stealth-chain. Other blocks of the same sender are written to the same stealth-chain by the receiver.

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

[71] NIST | Post-Quantum Cryptography: https://csrc.nist.gov/Projects/Post-Quantum-Cryptography/Round-2-Submissions
[72] Monero Stealth Address: https://getmonero.org/resources/moneropedia/stealthaddress.html

5.3.3 Confidential Transactions

The goal of confidential transactions[73] is that both the amount transferred, as well as, the account balance remains untraceable to outsiders. That's made possible by generating *commitments* for those values. These commitments can perform arithmetic operations (addition and subtraction). So if a commitment to the number three (3) and a commitment to the number five (5) are 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.

Blinding factors allow for a variance for each commitment without lifting the arithmetic properties. For technical feasibility analysis with confidential transactions and blinding factors for the desired data structure, a prototype of the commitment scheme has already been developed.

5.3.3.1 Zero-Knowledge Proofs

With zero-knowledge proofs, information can be verified without the information itself being disclosed: Alice proves to Bob that she is indeed in possession of some piece of knowledge without revealing any of that knowledge. The concept has been around since ~1985. Zero-knowledge proofs are a general concept and not limited to a specific cryptosystem.

A zero-knowledge proof must satisfy three properties:

- *Completeness*: If the statement is true (e.g., I have enough balance), the honest verifier will be convinced of this fact by an honest prover.
- *Soundness*: If the statement is false (e.g., I don't have enough balance), no cheating prover can convince the honest verifier that it is true, except with some small probability.
- *Zero-knowledge*: If the statement is true, no verifier learns anything other than the fact that the statement is true.[74]

5.3.3.2 Interactive vs. Non-interactive Zero-Knowledge Proofs

There are two ways in which zero-knowledge proofs can be achieved: *Interactive* and *non-interactive*. With interactive proofs, the prover and verifier must exchange information. The outcome of the proof convinces only the prover P_1 and the verifier V_1. If this check is to be carried out by the prover P_1 with another verifier V_2 they have to perform the proof again. Therefore, interactive zero-knowledge proofs are limited in transferability, which makes them impractical for a distributed network.

In a distributed network we need a kind of zero-knowledge proof, where the prover can show the result, and another party (the verifier) can verify the proof themselves. These are called non-interactive zero-knowledge proofs.[75]

5.3.3.3 Non-interactive Zero-Knowledge Range Proofs

Range Proofs are a concrete form of zero-knowledge proofs and allow for proving that a number is within a specific range. With Tixl, this is used to check that no negative amounts are sent and that no chain on the DAG can have a negative balance.

---

[73] Adam Gibson | An investigation into Confidential Transactions: https://github.com/AdamISZ/ConfidentialTransactionsDoc/blob/master/essayonCT.pdf
[74] Beampedia | Zero-knowledge Proof: https://www.beam.mw/beampedia-item/zero-knowledge-proof
[75] Tommy Koens et. al. | Efficient Zero-Knowledge Range Proofs in Ethereum: https://www.ingwb.com/media/2667860/zero-knowledge-range-proofs.pdf

5.3.3.4 Pedersen Commitments

A *commitment scheme* lets you keep a piece of data secret but commit to it so that you cannot change it later. A simple commitment scheme can be constructed creating a cryptographic hash of a piece of data combined with a so-called *blinding factor*. The blinding factor is like a random value preventing an outsider from revealing the piece of data when knowing the hash.

The Pedersen commitment scheme has the following properties:

- *Hiding*: A dishonest party cannot discover the honest party's value.
- *Binding*: A dishonest party cannot open their commitment in more than one way.
- *Non-correlation*: A dishonest party cannot commit to a value that is in some significant way correlated to the honest party's value.[76]

A Pedersen commitment has an additional property: Commitments can be added. The sum of a set of commitments is the same as a commitment to the sum of the data, with a blinding factor (BF) set as the sum of the blinding factors.

$$C(BF1,\ number1)\ +\ C(BF2,\ number2)\ =\ C(BF1+BF2,\ number1\ +\ number2)$$ [77]

Of course, a Pedersen commitment generated on an elliptic curve is not fully protected against quantum computers if they can solve the *Elliptic Curve Discrete Logarithm Problem* (ECDLP). Pedersen commitments are perfectly hiding but computational binding. That means that even if the cryptosystem is broken, the data on which the commitment was given cannot be revealed.

5.3.3.5 zk-SNARKs

"The acronym zk-SNARK stands for 'Zero-Knowledge Succinct Non-Interactive Argument of Knowledge' and refers to a proof construction where one can prove possession of certain information, e.g. a secret key, without revealing that information, and without any interaction between the prover and verifier. [...] In order to have zero-knowledge privacy [...], the function determining the validity of a transaction according to the network's consensus rules must return the answer of whether the transaction is valid or not, without revealing any of the information it performed the calculations on. This is done by encoding some of the network's consensus rules in zk-SNARKs. At a high level, zk-SNARKs work by first turning what you want to prove into an equivalent form about knowing a solution to some algebraic equations."[78]

5.3.4 Private Transactions Visualized

In this chapter, the technical infrastructure of Tixl is explained in detail concerning the interaction of its different components (DAG, account-chain, stealth-chains, NTRU, XMSS, etc.). Tixl is using a DAG as the underlying data structure. The account-chain and stealth-chains are realized on top of this, and they are more a semantic view of the transactions on the DAG. These semantic chains also provide information about who is allowed to append a new block to its predecessor.

Figure 2 shows what the DAG could look like after the first transactions. It shows an example where Alice receives TXL from the Genesis account (or Tixl distribution account), sends TXL to Bob and finally receives some TXL back from Bob.

---

[76] Commitment Schemes: https://github.com/adjoint-io/pedersen-commitment
[77] Pedersen Commitment: https://www.beam.mw/beampedia-item/pedersen-commitment
[78] What are zk-SNARKs?: https://z.cash/technology/zksnarks/

The Genesis account G creates a send transaction S to Alice account A. Alice then creates a receive block R on her stealth-chain GA. In addition, Alice stores a reference to the created stealth-chain GA in her account-chain A. Alice can send directly from the stealth-chain GA to Bob. Therefore Alice creates a send block on the stealth-chain GA. Since it is the first transaction Bob receives from Alice, Bob creates a corresponding stealth-chain AB and stores the reference on his account-chain B.

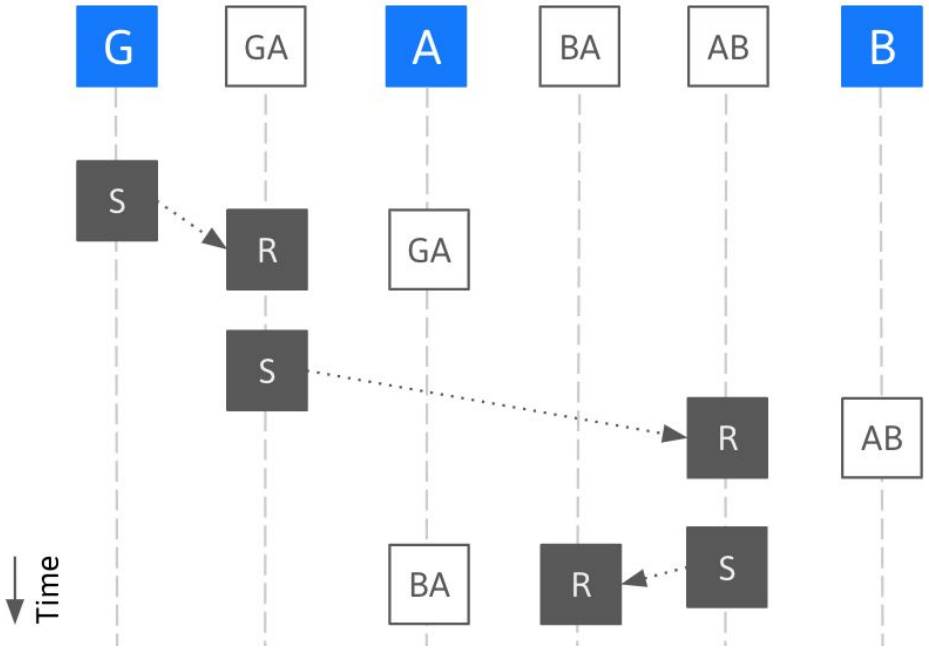

Figure 2: Tixl DAG with account-chains (G, A, B) and stealth-chains (GA, BA, AB)

A stealth-chain cannot be assigned to an account-chain by an outsider. Since the transactions are received on stealth-chains and the amounts are never transferred to an account-chain, the recipient is completely protected. Since the receiver is protected, the sender is also protected because the send block is saved on the stealth-chain as well. Only the Genesis account can be identified as the sender, because it does not send from a stealth-chain. That is of course not a problem, but even desirable.

To ensure that only an owner can write a new block on their chain, blocks are verified by signatures. Tixl currently uses XMSS for signatures to be prepared for the advent of quantum computers.

Tixl wants to provide the highest standard of privacy. Therefore it is inevitable that the amounts and balances are already encrypted before they will be sent to the network. For amount and balance encryption, NTRU will be used. NTRU is known for its speed and efficiency and was already used for business application over the last ten years while being protected under patent. A third party will be able to verify transactions by zero-knowledge proofs.

For zero-knowledge proofs, Tixl uses Pedersen commitments which may be replaced by another scheme at a later date. To guarantee maximum privacy, Tixl offers the possibility of carrying out *cut-through transactions* using zk-SNARKs.

5.3.5 Scalability

Since encryption and decryption take time, it's important to have the performance of the utilized algorithms in mind when building a cryptocurrency that needs to scale up to thousands of transactions per second. As soon as the Tixl prototype reaches a state allowing to measure times for encryption,

signing, decryption, and validation, this whitepaper will be updated with more information about those impacts on Tixl's scalability.

Also, it must be considered that there are new stealth-chains for every sender/receiver combination. Now, if a Tixl user wants to send a larger amount of TXL and needs to merge funds of several stealth-chains, this would take the regular encryption time per block times the number of stealth-chains. Having different solutions for this problem in mind, an easy solution for the start can be to have a clean-up feature implemented by wallets. Wallets would transfer and merge funds to a single stealth-chain when idling.

5.4 Consensus

The Tixl consensus algorithm can determine which transactions are valid and which to discard.

5.4.1 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 node can be executed by any natural or legal person without permission. Together all nodes form the Tixl network.

Nodes are needed to perform transactions in general. They transmit payments from the sender to the recipient. Also, 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.

A further essential 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 the consensus algorithm.

5.4.2 How do Tixl Nodes Reach Consensus?

Many of the existing consensus algorithms, like *Proof of Work* (PoW)[79] or *Proof of Stake* (PoS)[80], 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. So instead Tixl nodes reach consensus by utilizing the *Stellar Consensus Protocol* (SCP).

SCP "is a federated Byzantine agreement system that allows decentralized, leaderless computing networks efficiently to reach a consensus outcome on some decision."[81] An explanation is given in the following subchapters starting with the root issue, the Byzantine generals problem, because of which SCP was created.

5.4.2.1 The Byzantine Generals Problem & Byzantine Agreement

The name of the Byzantine general problem comes from a paper[82] from 1982 written by Leslie Lamport. Together with two co-authors, Lamport described the following allegory for the problem of

[79] Binance | Proof of Work (PoW) Consensus Algorithm:
https://www.binance.vision/blockchain/proof-of-work-explained
[80] Binance | Proof of Stake (PoS) Consensus Algorithm:
https://www.binance.vision/blockchain/proof-of-stake-explained
[81] Bob Glickstein | Understanding the Stellar Consensus Protocol:
https://medium.com/interstellar/understanding-the-stellar-consensus-protocol-423409aad32e
[82] Leslie Lamport et. al. | The Byzantine Generals Problem:
https://people.eecs.berkeley.edu/~luca/cs174/byzantine.pdf

decentralized decision making: The night before a possible battle, a group of Byzantine generals tries to decide whether to attack together or retreat. Messengers exchange the messages between the generals. Now there is a problem: Some generals and also messengers could be traitors. These traitors would be interested in sabotaging the generals' plans. Accordingly, the loyal generals must find a way to reach consensus.

If the Byzantine generals problem is now transferred to a network of servers that should agree on the validity of transactions, the servers can be defined as *Byzantine nodes*. Finding consensus within a group of Byzantine nodes can be defined as *Byzantine agreement*.

5.4.2.2 Federated Byzantine Agreement (FBA)

Majority based Byzantine agreement systems are vulnerable to so-called *Sybil attacks*. That is an attack where the attacker tries to control a peer network by creating or stealing a large number of fake identities. The goal of this attack can be, for example, to sabotage majority decisions. The idea of *federated Byzantine agreement* (FBA) is to defeat those attacks by introducing *decentralized quorum selections*. SCP is a certain kind of FBA system.

5.4.2.3 Stellar Consensus Protocol (SCP)

David Mazières introduced SCP in a whitepaper[83] 2015. Even though SCP is not tied to financial transactions, this explanation uses financial transactions as an example as they are most relevant for Tixl.

SCP uses *federated voting* to discover whether a network of (Byzantine) nodes can agree on a set of transactions. In a round of federated voting, each node must accept one or more possibly valid transactions as an outcome of that round. It can only do so if it's sure that other nodes in the network will not accept different transactions. That can be ensured by exchanging different types of messages with other nodes in the network. But what does "other nodes in the network" actually mean? To understand that, two main terms of SCP are introduced: *Quorum slices* and *quorums*.

A quorum slice is always viewed from the perspective of a node itself and designates a set of nodes that node trusts. A quorum slice must also contain the node itself. Each node can have multiple quorum slices. As by definition of SCP "a quorum slice represents a large or important enough set of peers that the node selecting the quorum slice believes the slice collectively speaks for the whole network."[84]

A quorum can be defined as a non-empty set of nodes containing at least one quorum slice of each of its members. For example, given the nodes $n1,\ n2,\ n3,\ n4$ have the following quorum slices:

$$
\begin{aligned}
n1 &= \{ n1,\ n2,\ n3 \} \\
n2 &= \{ n2,\ n3,\ n4 \} \\
n3 &= \{ n2,\ n3,\ n4 \} \\
n4 &= \{ n2,\ n3,\ n4 \}
\end{aligned}
$$

In this case $\{ n2,\ n3,\ n4 \}$ would form a quorum because it contains a quorum slice for each of its members. If a quorum also containing $n1$ should be formed this would have to include all nodes $\{ n1,\ n2,\ n3,\ n4 \}$.

[83] David Mazières | The Stellar Consensus Protocol: A Federated Model for Internet-level Consensus: https://www.stellar.org/papers/stellar-consensus-protocol.pdf
[84] David Mazières | The Stellar Consensus Protocol (SCP): https://tools.ietf.org/html/draft-mazieres-dinrg-scp-03

Back to the federated voting and to an example: Given one payment transaction is sent to a network of nodes and those nodes want to find an agreement on whether this transaction is valid or not. Now, a node receiving the transaction optionally begins by casting a *vote* for the transaction validity. It broadcasts the vote itself, its quorum slices and also its identifier within one message to the network. A node receiving broadcasted messages from other nodes can traverse the quorum slices. If it finds a quorum of nodes that vote for the same outcome, it can now *accept* that outcome and broadcast this information to the network as well. To finish the federated voting process for one transaction, a node must wait for a quorum of nodes all accepting it and can then *confirm* the outcome.

Of course, situations can arise in which it is not immediately possible to find a quorum for a decision. In order to be able to perform federated voting nevertheless, the network must fulfill the *quorum intersection* property. In a network, which fulfills this property, any two quorums overlap in at least one node. This property and some other edge cases are explained in detail in the Stellar whitepaper. Furthermore, the Tixl consensus algorithm, based on SCP, will be made available open source, so code examples for handling such cases will follow in 2019-2020.

5.4.3 Does every Tixl Node need to know All Transactions?

A Tixl node can be operated with different configurations. Either a node stores the whole 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 one transaction were 1 kilobyte, the entire ledger would already be 100 gigabytes with 100 million transactions.

As part of the Tixl node incentive program, historical nodes will receive compensation in TXL for their computing services.

5.4.4 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 increase motivation, 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 contributes to the stability of the Tixl network.

5.4.5 Will Tixl be 100% Decentralized from the Start?

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

5.4.6 Scalability

Fortunately, due to Tixl's data structure, the consensus algorithm only has to vote for conflicting transactions. In case a valid transaction is sent to the network, nodes can persist the transaction on the ledger and broadcast it to other nodes. Since SCP is known to establish consensus within a few seconds, even if there are some more conflicting transactions, nodes will still be able to reach consensus quickly. It's also known, that SCP can deal with high transaction volumes. Although there is

no verified statement from the Stellar foundation, there are rumors that SCP can handle 10,000 transactions per second in certain network constellations.[85]

[85] Kyle McCollom | How Many Transactions Per Second Can Stellar Process?: https://www.lumenauts.com/blog/how-many-transactions-per-second-can-stellar-process

6 Roadmap

The development of Tixl started in 2018. The focus during this time was on the preparation of the whitepaper, the legal preparations and the development of a prototype. The following roadmap shows the next steps of Tixl's development.

Because the outcome of the token sale has a major impact on the project, the roadmap may change in the future. Changes or other updates regarding the roadmap will be published on Tixl's social media channels as well as via email for those who signed up on the Tixl website.

Q2 2019

- First phase of fundraising, Pre-IEO
- Internal ledger prototype release
- External whitepaper audit & result incorporation
- Kickoff consensus algorithm development
- Kickoff API gateway development
- Pitch at ANON Blockchain Summit Austria
- Pitch at Bankingclub Cologne, Germany
- Release of the first press article
- Listings on ICO/IEO websites
- Creation of VC compatible pitch deck, dispatch to at least 100 VCs
- Approaches to at least 100 private investors and business angels

Q3 2019

- Second phase of fundraising, Pre-IEO
- Internal consensus prototype release
- Internal API gateway prototype release
- Kickoff Tixl web wallet development
- Attendance on at least one conference as a speaker or for a pitch
- Release of three more press articles
- Creation of detailed paper about Tixl's technology stack
- Depending on Q2 approaches to more potential investors
- Transfer of the ledger prototype to a production-ready version

Q4 2019

- Third phase of fundraising, IEO
- Security audit of the Tixl ledger by external experts
- Transfer of the consensus algorithm prototype to a production-ready version
- Transfer of the API gateway to a production-ready version
- Attendance on at least one conference as a speaker or for a pitch
- Beta test of the full Tixl software stack (ledger, consensus, API gateway, web wallet)
- List MTXLT on at least one regulated exchange
- Approaches to potential advisors from the industry
- Approaches to potential business partners for Tixl as a payment method, this includes payment providers, exchanges and banks
- Improvement of the Tixl web wallet
- Start of first marketing bounty campaigns where MTXLT are used as compensation

Q1 2020

- Fourth phase of fundraising
- Stress test of Tixl's software stack in a private network
- Another security audit, this time of the full Tixl software stack
- Focus on deals with business partners approached in Q4 2019
- Bug fixes and performance improvements for all of Tixl's software parts
- Assembly of an advisory board with people approached in Q4 2019

Q2 2020

- Fifth and last phase of fundraising
- Announcement of the token swap date
- Stress test of Tixl's software stack in an open beta
- Start of first development bounty campaigns where MTXLT are used as compensation for programming software parts like e.g. desktop wallets

Q3-Q4 2020

- Execution of Tixl's token swap
- Tixl network launch
- Support of business partners integrating Tixl in their infrastructure
- Start to decentralize Tixl by slowly adding the first external nodes to the consensus algorithm

Since the concrete task packages in the future depend strongly on the success of the token sale, the stages in 2021 and 2022 are formulated here rather as goals and are to be understood also in such a way.

2021

- Tixl is now within the top 5 of all privacy coins in terms of market cap and trading volume
- Tixl is listed on different major exchanges and integrated into well-known payment providers

2022

- Tixl is now within the top 2 of all privacy coins in terms of market cap and trading volume

6.1 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 Tixl's early investors.

6.2 Marketing Plan

The marketing plan for Tixl can be roughly divided into two parts, firstly the marketing for fundraising and secondly the marketing for Tixl as the currency itself. Since the reasonability of possible marketing efforts depends on external factors, planning can change at any time. It's therefore not to be understood as final.

6.2.1 Fundraising Marketing Plan

Marketing for fundraising can be divided into a sequence of several steps. These steps are explained in Table 3. The first column of Table 3 shows the period in which a marketing effort, shown in the second column, will be performed.

Period	Marketing Efforts
May 01-12 2019	At the start of the fundraising, free marketing efforts will be initiated. That includes, for example, addressing business angels from Tixl's network. Not only does this serve possible sales of Tixl tokens but also it will provide valuable feedback for later VC pitches. At the same time, it is planned to bring the Tixl ICO/IEO to websites specialized in those listings. That was already done for the airdrop and generated about 5,000 registrations without investing any funds. Furthermore, Tixl will be shared and discussed on various forums during this period. This channel serves more to generate feedback from the crypto community.
May 13-31 2019	Marketing in the second half of May will begin with participation in the German event "INNOVATIONSforBANKS 2019". Tixl will be presented to representatives of the German banking industry. The medium-term goal of the event is to establish partnerships with banks. In addition, offers from companies or freelancers who have already successfully marketed token sales are to be obtained during this period. These offers will then be compared at the end of the month. If there is an attractive cost-benefit ratio for a provider, he is commissioned to support Tixl's marketing efforts.
June 01-30 2019	During this period, paid promotions for the token sale will take place for the first time. Depending on the outcome of the previous month, these will take place in consultation with the marketing partner. In this phase, offers from crypto websites and influencers are obtained and evaluated. On the basis of various factors, it is decided whether and which promotions will be placed. The second fundraising phase starts on July 1. Accordingly, marketing will concentrate on the launch of this phase during this period.
July - End of Fundraising 2019/20	Marketing for the further fundraising phases cannot yet be planned. The strategy depends strongly on the outcome of the first two fundraising phases. As soon as these results are available, this marketing plan will be updated accordingly.

Table 3: Fundraising Marketing Plan

6.2.2 Currency Marketing Plan

In comparison to the marketing plan for fundraising, it makes little sense at the moment to schedule possible marketing measures for Tixl as a currency itself. Nevertheless, there is already a basic strategy for the marketing of Tixl as a currency, which is described in the following chapters.

6.2.2.1 Marketing via Listings on Regulated Exchanges

It may sound logical, but for the sake of completeness marketing by exchange listings shall be briefly described here. The aim is to list Tixl on regulated exchanges with large trading volumes. Only if the majority of cryptocurrency users can acquire tixl, Tixl can establish itself as an asset.

6.2.2.2 Marketing via Payment Providers

There are already various providers for receiving and sending payments in cryptocurrencies.[86] Since Tixl is intended to be widely used as a common means of payment, integration into existing payment providers is crucial. The development of an own payment service, exclusively for Tixl, is neither meaningful nor does it fit the corporate purpose of Tixl gGmbH.

6.2.2.3 Marketing via Banks

In addition to integration into exchanges and payment providers, Tixl is also striving to achieve partnerships with banks. Some banks already offer their customers the opportunity to purchase cryptocurrencies such as Bitcoin via their account. If banks provided their customers the option to acquire Tixl, this would improve the distribution outside the cryptocurrency scene itself. That is more a long-term goal of Tixl.

6.2.2.4 Marketing via Onboarding of Well-Known Advisors

When potential investors investigate new cryptocurrencies they always take a look into the team and their advisors. An advisor does not always have to be a specific person, but can also represent a company. If behind a team there are very well-known advisors who have a highly respected image in public, this makes the marketing of a cryptocurrency a lot easier.

At the same time, the willingness of a consultant to stand behind a team is also a sign of quality. Because if someone who knows a scene very well agrees to represent a team as an advisor publicly, this supports the plausibility and potential of a project.

6.2.2.5 Marketing via Bounties

As already briefly explained in chapter 3.4, bounties are about the assignment of tasks to people outside the team. The payment is made in the issued cryptocurrency, in this case, Tixl itself. Exactly this feature makes bounties attractive at all.

Vesting periods[87] can be used to prevent participants in bounty campaigns from selling their tokens directly afterward.

6.3 Updates / Communication

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

[86] Sudhir Khatwani | 7 Popular Bitcoin Payment Gateways For Merchants: https://coinsutra.com/bitcoin-payment-gateways-merchants/
[87] Time a bounty campaign participant has to wait before they may sell their tokens.

7 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.

7.1 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.

7.2 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.

7.3 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.

7.4 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 cryptocurrency will be much more difficult in just a few years.

7.5 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.

7.6 Risk from Conflicts of Interest

There are personnel and capital links between the partners involved in this 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 those decision-making situations will be resolved to the detriment of the Tixl project.

7.7 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.

7.8 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.

7.9 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. Therefore, it is 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.

7.10 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.

7.11 Reputational Risk

It is possible that the reputation of FinTechs, (large) cryptocurrencies, as well as ICOs/IEOs, may deteriorate with individual interest groups or in society as a whole, e.g. due to a large number of unrealized 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.

Tixl Glossary

Tixl Ledger
The ledger contains the entire Tixl transaction history.

Tixl Network
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 currency unit used in Tixl.

MTXL
1,000,000 (one million) TXL. MTXL is also supposed to be used as a shortcode or symbol on exchanges.

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

MTXLT
1,000,000 (one million) TXLT

General Glossary

Airdrop
In an airdrop, tokens of a cryptocurrency are given away free of charge.

Blockchain
A blockchain is an append-only ledger of transactions, represented by a chain of blocks where each block references its predecessor.

Bounties
Bounties are campaigns or programs in which tasks are given to people outside the team (the community) and remuneration is in tokens. For Tixl, developer bounties as well as marketing bounties are considered.

Bounty Campaign Vesting Period
Time a bounty campaign participant has to wait before they may sell their tokens.

BTC
BTC is the currency shortcode or symbol for Bitcoin.

Circulating Supply
The quantity of a currency in circulation.

Cryptocurrency
A cryptocurrency is a digital asset that can be used as an alternative medium of exchange to classic currencies such as the US-Dollar or Euro. [88]

Directed Acyclic Graph (DAG)
A Directed Acyclic Graph is an alternative data structure to the established blockchain for a decentralized ledger.

Discord
Discord is an online messaging platform.[89]

ECDLP
ECDLP is the abbreviation for Elliptic Curve Discrete Logarithm Problem. The difficulty of solving the discrete logarithm problem is essential for security.[90]

EOS
EOS is the currency shortcode for the native asset of the eosio infrastructure for decentralized applications.[91]

[88] Cryptocurrency: https://en.wikipedia.org/wiki/Cryptocurrency
[89] Discord Messaging Platform: https://discordapp.com
[90] Discrete Logarithm Problem: http://wiki.c2.com/?DiscreteLogarithmProblem
[91] eosio: https://eos.io

EUR
EUR is the currency shortcode or symbol for the Euro.

Federated Byzantine Agreement (FBA)
In Federated Byzantine Agreement systems, each node does not have to be known and verified ahead of time, membership is open, and control is decentralized. Nodes can choose who they trust. System-wide quorums emerge from decisions made by individual nodes.[92]

Fiat Money
Fiat money usually refers to classic currencies such as the US-Dollar or the Euro.[93]

ICO
ICO 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.

IEO
IEO is the abbreviation for Initial Exchange Offering. An IEO is an ICO where tokens are sold through an exchange.

Market Cap
Market Cap stands for Market Capitalization and describes the total value of all tokens/coins/units of a currency.

Proof of Work (PoW)
Proof of Work is a consensus algorithm used e.g. by Bitcoin, to decide which transactions are valid will be persisted in the blockchain. "In Proof of Work, in order for an actor to be elected as a leader and choose the next block to be added to the blockchain they have to find a solution to a particular mathematical problem."[94]

Proof of Stake (PoS)
"Proof of Stake (PoS) is a category of consensus algorithms for public blockchains that depend on a validator's economic stake in the network."[95]

Delegated Proof of Stake (DPoS)
Delegated Proof of Stake is based on Proof of Stake but with the validators being delegated and elected by token holders.

Quantum Computing
Quantum computing is the use of quantum-mechanical phenomena such as superposition and entanglement to perform computation. 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

---

[92] Shaan Ray | Federated Byzantine Agreement: https://towardsdatascience.com/federated-byzantine-agreement-24ec57bf36e0
[93] Fiat: https://en.wikipedia.org/wiki/Fiat_money
[94] Georgios Konstantopoulos | Understanding Blockchain Fundamentals, Part 2: Proof of Work & Proof of Stake: https://medium.com/loom-network/understanding-blockchain-fundamentals-part-2-proof-of-work-proof-of-stake-b6ae907c7edb
[95] Ethereum Proof of Stake FAQ: https://github.com/ethereum/wiki/wiki/Proof-of-Stake-FAQ#what-is-proof-of-stake

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. Peter Shor invented an algorithm (named Shor's algorithm), which uses the suspected power of a quantum computer to solve the factorization problem.[96]

USD
USD is the currency shortcode or symbol for the US-Dollar.

Volatility
Volatility is a measure of how much the price of an asset varies over time.[97]

[96] Quantum Computing: https://en.wikipedia.org/wiki/Quantum_computing
[97] The Bitcoin Volatility Index: https://bitvol.info/index.html