Tixl Whitepaper

Christian Eichinger christian@tixl.me
Sebastian Gronewold sebastian@tixl.me
Bernd Strehl bernd@tixl.me

Version 11 - November 2019
This document is available free of charge from:
https://tixl.me/whitepaper

Executive Summary

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

The Problem
None of the popular digital assets allow private, instant and zero-fee transactions at the same time. But why is that a problem? In a world headed more towards digital currencies, we must secure and preserve the essential properties of traditional money. No one wants the public to be able to look into their monetary transactions, whether they are governments, companies or private people. In addition, all users of a digital asset want to pay the lowest fees possible - the higher the fee, the lower the potential for widespread adoption. Last, but not least, if a future digital asset is slow in terms of transaction speed, it's not a future digital asset.

The Solution
Tixl uses the most sophisticated technologies to have emerged from the blockchain world over recent years. It uses a Directed Acyclic Graph (DAG) data structure together with the Stellar Consensus Protocol (SCP) to support fast transactions. Tixl also uses Zero-knowledge proofs with a commitment scheme to enable confidential transactions (hiding transaction amounts). To protect transaction senders and receivers, Tixl uses stealth addresses and coin shuffling. Also, to ensure that transactions stay private in the future, quantum secure or upgradable cryptosystems are implemented to encrypt transaction details.

Mining Free
Traditional mining, as used with Bitcoin, damages Earth's environment. Tixl's solution does not involve energy-intensive algorithms. Instead, Tixl's consensus algorithm is based on a network of decentralized nodes which vote for, or against, transactions. Each node can decide which other nodes it trusts. The long-term goal is to have a network of different institutions hosting Tixl nodes all over the world. Nodes are paid for with a certain percentage of the total token supply and they should be intrinsically motivated if they hold a large amount of Tixl tokens, or have a business model based on processing Tixl transactions.

Fundraising
To finance the development and implementation of Tixl and raise capital for marketing, a token sale is being conducted. During the fundraising period, Tixl BEP2 Tokens [MTXLT] on the Binance Chain, are sold and operate as vouchers that can later be swapped for Tixl. We began the third phase of our Tixl token sale on October 18, 2019. As a recap: The first two phases of the token sale have been completed — raising 450,000 USD in phase 1 and 800,000 USD in phase 2. The total amount raised so far is 1,250,000 USD.

https://medium.com/tixlcurrency/tixl-token-sale-phase-3-official-start-41a9f0ee504c

Investment Potential
Investing in Tixl provides opportunities, and risks, similar to investing in Bitcoin, Ethereum or other digital assets. If Tixl rises in price over time, 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 digital asset in which the digital asset can provide 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 - via 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.
- No transaction fees - 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 leads to criticism, by cryptocurrency proponents, of the traditional banking system. Problems with these monetary systems occur repeatedly in emerging markets where inflation spirals out of control and there are declines in the exchange rate of the national currency. This is currently evident in Argentina and Venezuela, among others. Large, developed, industrial nations are not immune to these effects either, as observed with the financial crisis triggered in 2008 in the USA.

The crypto revolution started with Bitcoin. Inspired by the possibilities of building a decentralized and self-sufficient network, aspects of existing solutions were improved on again and again. For example, Zcash[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 still no digital asset that can properly satisfy all three properties of privacy and speed, with a lack of transaction fees. Tixl is designed to be one of the first digital assets to have all of these characteristics. By deliberately avoiding features like smart contracts, Tixl is focused solely on the requirements of payment transactions.

[1] Fiat money: https://en.wikipedia.org/wiki/Fiat_money
[2] Zcash cryptocurrency: https://z.cash

Table of Contents

1. Introduction

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

1.1 Tixl Explained in 3 Sentences

The Tixl project is about creating a digital asset - also named Tixl - that focuses on private and instant transactions that are free of fees. Tixl accomplishes this by utilizing a unique mix of 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 outlined in the glossary, the currency shortcode (symbol) for Tixl is TXL.

1.2 Motivation for Developing Another Digital Asset

Over 3,000 tokens are currently listed on coinmarketcap.com[3]. Only a few of these tokens pursue the goal of establishing themselves as an actual means of payment. A large number of them can be classified as utility tokens for a new applications on an existing platform like Ethereum[4]. Currently, the use of ERC-20 Tokens[5] on the Ethereum blockchain seem to be the most common. In addition, BEP2[6] tokens based on Binance Chain[7] are gaining in popularity.

Tokens based on proprietary technical solutions have very different focal points. In particular, the following trend topics appear most commonly:

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

[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
[6]BEP2 Token: https://github.com/binance-chain/BEPs/blob/master/BEP2.md
[7]Binance Chain: https://docs.binance.org

Due to the technical implementation of existing solutions, no digital asset has yet been able to effectively achieve the ideal combination of privacy, zero-fee transactions and high transaction speed in a sufficiently collaborative manner. For this reason, Tixl provides its technical solution, focusing on payments only.

Why is the combination of attributes above so important for a digital asset? Firstly, the world is increasingly headed toward digital currencies. All of these currencies have got common stakeholders distributed worldwide - governments, companies, and private citizens. If a digital asset like Tixl is to succeed in becoming a mainstream store of value, it needs to contain specific properties to fulfill the requirements of its stakeholders.

Importantly, all stakeholders want the transactions made with a digital asset 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 digital asset, having zero transaction fees (or at least very low fees) is also an important criterion. This is especially important when making payments within one country, and not across borders - people expect these payments to be free of charge. Introducing high transaction fees for a new digital asset would be a step backward in comparison to Fiat money. Also, in an age when it is possible to send messages, pictures and videos all over the world in a matter of seconds, the ability to send digital assets at speed will become a standard requirement.

1.2.1 Motivation for Privacy

Tixl is not the first digital asset to address the need for private transactions. The number of popular privacy coins currently on the market proves that privacy is a sought after characteristic of digital assets. Among the top 30 tokens, Monero, Dash and Zcash, for example, all focus on private transactions.

The potential for the transfer of payments within business environments, as well as private life, is huge. The following two examples illustrate this.

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 digital payments. Alice pays the whole bill, so Bob then owes her $15. Both are enthusiastic about digital assets 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 her current balance, on the decentralized ledger.
- Bob doesn't want to pay high transaction fees to send money to Alice.

So, both want the digital asset to function as if $15 had been handed over 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.

Example: Point of Sale & E-Commerce

Alice and Bob go to a burger restaurant together where the restaurant already accepts digital assets as a means of payment. Both the restaurant operator and the customers have differing requirements for the use of digital assets:

- Payments should be completed quickly (within a few seconds).
- The restaurant does not want Alice or 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 their other transactions on the decentralized ledger.

The restaurant, as with Alice and Bob, wants the digital asset 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. Also, neither the restaurant nor Alice and Bob would be able to see the other transactions they have each made. On top of this, the transaction would settle instantly. In the case of non-private digital assets such as Bitcoin, the competition can view all transactions going to the public address of a competitor and easily work out:

- How many different customers pay with Bitcoin?
- How often these customers purchase?
- Whether there are customers in common because both companies have been paid from the same Bitcoin address.
- How many Bitcoins the competitor currently holds and how quickly, or regularly, these Bitcoins are exchanged with fiat currencies. As a result, it may even be possible to draw conclusions about liquidity.

Potentially, there may be mixing services or payment providers optimizing the privacy of merchants trading in existing digital assets. Nevertheless, as one of the latest Amazon patents[8] shows - an open data structure, which does not have privacy in its core, opens the door for companies interested in payment data.

[8]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/

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 relatively low at the beginning of the project. Therefore, the MTXL was 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 displayed as 900,000 MTXL.

1.4 How was the Total Supply Determined?

The total supply of 900,000 MTXL was picked due to psychological reasons which are relevant during the first years of marketing. With 900,000 MTXL being available, 1 MTXL can have the same value as 1 BTC, whilst only having approximately 4 percent of its market cap[9]. Consequently, the value of 1 MTXL can be high when compared to Bitcoin or other digital assets. Limiting the amount of MTXL to this low supply may increase demand, and this may lead to a higher price.

Later, as TXL is viewed not only as an investment opportunity, but also as a viable means for purchasing goods, exchanges can continue to display the price of 1 MTXL but shops can show prices of products in TXL. For example, if Tixl had a market cap of $90,000,000,000[10], this would mean that 1 TXL equals $0.10[11]. If a product in a supermarket costs $1 in Tixl, it would cost 10 TXL. In comparison to other digital assets, which in most cases have fewer tokens, this has much better real-world application 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."[12] The digital asset market is volatile because large trades can result in significant price movements. This is due to the total market cap of all digital assets (measured in USD) being much lower than that of less volatile investments (e.g. gold). This results in a chicken-and-egg dilemma because it is this very price instability that keeps potential investors away, and limits the growth of the digital

[9] The exact percentage depends on the circulating supply of both Bitcoin and Tixl.
[10] $90,000,000,000 approximates the Bitcoin market cap as at April 13, 2019.
[11] If all available TXL were in circulation. In all probability, the circulating supply will remain lower for the foreseeable future.
[12] The Bitcoin Volatility Index: https://bitvol.info/index.html

asset market cap.[13] Not only does this hold potential investors back, it also prevents digital assets from being used as a wide-spread medium of exchange and store of value.

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

[13] 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 increased digitization of traditional banking business. In particular, start-ups in this market known as FinTechs are ensuring ongoing innovation and increasing the pressure on conventional banks. For online purchases, payment providers such as Stripe and PayPal have established themselves ahead of traditional banks. The two IT giants, Apple and Google, are pursuing the goal of further digitizing payment transactions and making it extremely convenient to make these payments via smartphones.

With the creation of Bitcoin and the invention of blockchain technology, it became possible to transmit values in a decentralized network without a central authority. The age of cryptocurrencies - or digital assets - was born. Cryptocurrencies do not stop at national borders, and their value is determined worldwide, similar to commodities such as gold. Inspired by the possibilities of building a decentralized and self-sufficient network, aspects of existing solutions have continued to be built upon. For example, Zcash is based on Bitcoin and has added the element of privacy. 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 start of the internet age, most people thought they were anonymous because they sat behind an IP address. As we know today, this is a pseudo-privacy. We have a similar situation with Bitcoin with its public addresses. 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 can discover relevant information. In the same way privacy was necessary for the internet in the beginning; it now becomes increasingly important for cryptocurrencies.

Due to the technical implementation of existing solutions, no digital asset has yet been able to effectively achieve the ideal combination of privacy, zero-fee transactions and high transaction speed in a sufficiently collaborative manner. For this reason, Tixl provides its technical solution, focusing on payments only. The following chapters compare Tixl to various existing cryptocurrencies, attaching particular importance to privacy coins.

2.1 Bitcoin

Bitcoin was the first widely used cryptocurrency. As a result, it has gained a dominant position and the highest degree of recognition. The myth surrounding the inventor Satoshi Nakamoto has certainly helped.

Symbol:	BTC
Form of organization:	Community-driven
Launched:	January 3, 2009
Fees:	$0.22 - $1.00[14] <*$0.01 (through Lightning Network*[15])
Transaction speed:	10-60+ Minutes (dep. on block confirmations) *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 learn from other approaches. Critics focus on 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 topics of concern. That is one of the reasons the Bitcoin community split up and Bitcoin Cash (BCH)[16], a Bitcoin (BTC) fork, was created in 2017.

The fact that mixing services have become more widespread and that there are recommendations to use a new Bitcoin address for each transaction shows that lack of privacy is a problem.

Ongoing Improvements

By creating the *Lightning Network*, the Bitcoin community invented an off-chain solution to tackle some of Bitcoin's scalability issues. It allows much faster, cheaper and a greater number of transactions per second, but comes with some trade-offs.[17]

Competition to Tixl

Bitcoin is not a direct competitor of Tixl. As Bitcoin does not support private transactions, nor has a scaling or fee reduction solution implemented in the core itself, Tixl will be technologically superior to Bitcoin. From the Tixl perspective, Bitcoin is considered "Digital Gold". Bitcoin and Tixl could co-exist as digital assets and stores of value having different properties.

[14] Bitcoin fees: https://bitcoinfees.info/
[15] Bitcoin Lightning Network fees: https://medium.com/suredbits/lightning-101-lightning-network-fees-86abbbc17024
[16] Bitcoin Cash: https://www.bitcoincash.org
[17] 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 or store of value. One can deploy so-called *smart contracts* on Ethereum. A smart contract is a program on the Ethereum blockchain which can, for example, represent agreements between different parties as computational code[18]. Besides, Ethereum allows issuing custom assets on their platform, which numerous teams have used to conduct ICOs over past years.

Symbol:	ETH
Form of organization:	Ethereum Foundation (non-profit)
Launched:	July 30, 2015[19]
Fees:	$0.11[20]
Transaction speed:	~15 Seconds (depending on fee spent)
Ledger type:	Blockchain
Cryptosystem for signatures:	Elliptic curve secp256k1
Consensus algorithm:	Proof of Work (Ethash) / Proof of Stake deployed on TestNet[21]

Downsides

Ethereum currently has weaknesses similar to Bitcoin.

Ongoing Improvements

As with Bitcoin, the most significant potential for improvement lies in scalability and the ability to conduct 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 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 of Tixl.

[18] 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

[19] Ethereum: https://en.wikipedia.org/wiki/Ethereum

[20] Ethereum transaction fees: https://bitinfocharts.com/de/comparison/ethereum-transactionfees.html

[21] 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 positioned 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 fast transactions. In addition to its own asset XRP, the Ripple platform also allows issuing and sending of other assets.

Symbol:	XRP
Form of organization:	Ripple Labs, Inc.
Launched:	2012
Fees:	$0.0005[22]
Transaction speed:	4 Seconds
Ledger type:	RippleNet[23]
Cryptosystem for signatures:	Elliptic curve secp256k1
Consensus algorithm:	Federated Byzantine Agreement (FBA)[24]

Downsides

Since anyone 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. Ripple's XRP website describes XRP as a bridge utility for exchanging value in different Fiat currencies around the globe[25]. There is also no privacy protection for transactions over that of Bitcoin.

Ongoing Improvements

Ripple is very active in its development of the XRP ledger. Currently, they are focusing more on stability than on larger features, at least in terms of what is publicly visible.

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 of Tixl. However, even if Ripple changed their marketing strategy, it would still not have the ability to conduct private transactions as a feature.

[22] Ripple/XRP transaction fees: https://bitinfocharts.com/de/comparison/xrp-transactionfees.html
[23] Ripple: https://ripple.com/
[24] Shaan Ray | Federated Byzantine Agreement: https://towardsdatascience.com/federated-byzantine-agreement-24ec57bf36e0
[25] Ripple on XRP: https://www.ripple.com/ripplenet/on-demand-liquidity

2.4 Stellar

Stellar is based on a fork of Ripple. The partnership with IBM, in particular, has made Stellar popular over recent years. Stellar uses a self-developed variation of the Federated Byzantine Agreement which supports very fast transactions. As with Ripple, it is possible to issue and send custom assets on the Stellar platform, as well as their own asset *XLM*.

Symbol:	XLM
Form of organization:	Stellar Development Foundation (non-profit)
Launched:	July 31, 2014
Fees:	0.00001 XLM [26]
Transaction speed:	3-5 Seconds[27]
Ledger type:	Stellar Network
Cryptosystem for signatures:	Elliptic curve ed25519
Consensus algorithm:	Stellar Consensus Protocol (SCP)

Downsides

Stellar currently suffers from the same weaknesses regarding private transactions as Ripple.

Ongoing Improvements

The Stellar foundation plans to improve the decentralization of the Stellar network whilst preserving performance.[28]

Competition to Tixl

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

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

2.5 Monero

Monero is considered the father of all privacy coins. To obfuscate the origin, 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.[29]

Symbol:	XMR
Form of organization:	Community-driven
Launched:	2014
Fees:	$0.023 [30]
Transaction speed:	4-26 Minutes (dep. on block confirmations) [31]
Ledger type:	Blockchain
Cryptosystem for signatures:	Elliptic curve ed25519 [32]
Consensus algorithm:	Proof of Work (CryptoNote)

Downsides

As with Bitcoin, Monero suffers from problems regarding transaction speed, scalability, and relatively high transaction 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 introducing second layer solutions.[33]

Competition to Tixl

Like Tixl, Monero targets private payments, so is a serious competitor. Of all the privacy coins, it currently has the highest market cap. Nevertheless, Monero's scaling problems allow Tixl to compete with it.

[29] Monero: https://www.getmonero.org/
[30] Monero Transaction Fees: https://bitinfocharts.com/de/comparison/monero-transactionfees.html
[31] Monero Transaction Speed: https://www.monero.how/how-long-do-monero-transactions-take
[32] Edwards25519 Elliptic Curve: https://monerodocs.org/cryptography/asymmetric/edwards25519/
[33] Monero Roadmap: https://www.getmonero.org/resources/roadmap/

2.6 Zcash

ZCash is a fork from Bitcoin but uses a different Proof of Work algorithm called Equihash. Unlike Monero however, the Zcash Ledger distinguishes between *transparent* and *shielded* addresses. This means Zcash can allow both private and public transactions on one ledger. To achieve privacy with shielded addresses, Zcash uses so-called "zero-knowledge proofs", specifically *zk-SNARKs*.[34] Zero-knowledge proofs are widely considered the most cutting-edge cryptography available.

A further positive development with Zcash is that the New York State Department of Financial Services has approved trading the privacy-protecting cryptocurrency.[35]

Symbol:	ZEC
Form of organization:	Zcash Foundation (non-profit)
Launched:	October 28, 2016
Fees:	$0.00000432 [36]
Transaction speed:	~2.5-15 Minutes (dep. on block confirmations)
Ledger type:	Blockchain
Cryptosystem for signatures:	Elliptic curve BLS12-381
Cryptosystem for encryption:	Elliptic curve BLS12-381[37]
Consensus algorithm:	Proof of Work (Equihash)

Downsides

With zk-SNARKs, Zcash currently offers arguably the strongest privacy on a publicly accessible ledger. Up until 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 made. Nevertheless, scalability will remain a major pain point for Zcash for the foreseeable future.

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

Early in 2019, an Equihash-compatible ASIC miner was announced by Bitmain, which opens up Zcash's future to miner centralization similar to Bitcoin.[38] That was one of the reasons Zcash was forked by one of their founding members who introduced a new privacy coin called Ycash[39].

[34] Griffin Knight | Monero vs. Zcash and the Race to Anonymity: https://medium.com/coinmonks/monero-vs-zcash-and-the-race-to-anonymity-4322b0a9bd90
[35] New York State | Department of Financial Services: https://www.dfs.ny.gov/about/press/pr1805141.htm
[36] Zcash Transaction Fees: https://bitinfocharts.com/de/comparison/zcash-transactionfees.html
[37] zk-SNARK Elliptic Curve Construction: https://z.cash/blog/new-snark-curve/
[38] Examples of pivacy coins: https://blog.liquid.com/examples-of-privacy-coins-monero-zcash-dash
[39] Ycash: https://ycash.xyz

Ongoing Improvements

According to what is discussed on meetups and at conferences, the Zcash team will concentrate on scalability over the next few years. Zcash's roadmap doesn't highlight other features.[40]

Competition to Tixl

Zcash is a direct competitor of Tixl and currently has the best privacy concept of all other cryptocurrencies. It has a lower market cap than Monero but a higher daily transaction volume. For Zcash, the same opportunities exist as for Monero, however the advantages in scalability make Tixl a strong competitor.

[40] 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 one to obscure the exact flow of each transaction.[41]

Symbol:	DASH
Form of organization:	Dash Core Group, Inc.
Launched:	January 18, 2014
Fees:	$0.0012[42]
Transaction speed:	~2.5-15 Minutes (dep. on block confirmations)[43] *almost instant through InstantSend*[44]
Ledger type:	Blockchain
Cryptosystem for signatures:	Elliptic curve secp256k1[45]
Consensus algorithm:	Proof of Work (X11)

Downsides

Dash claims to be decentralized, but the implementation of CoinJoin does not support this claim. 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 is entirely possible to reverse engineer PrivateSend transactions to reveal origin and destination details.

As with 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.

Ongoing Improvements

According to Dash's roadmap[46], the team will focus on improving its wallet software. 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 be-

[41] LIQUID | Examples of pivacy coins: https://blog.liquid.com/examples-of-privacy-coins-monero-zcash-dash
[42] Dash Transaction Fees: https://bitinfocharts.com/de/comparison/dash-transactionfees.html
[43] Dash Statistics: https://bitinfocharts.com/dash/
[44] Dash InstantSend: https://docs.dash.org/en/stable/wallets/dashcore/privatesend-instantsend.html
[45] Dash Public Key: https://github.com/dashevo/dashcore-lib/blob/master/docs/publickey.md
[46] Dash Roadmap: https://www.dash.org/roadmap/

hind Dash is very experienced in doing marketing for its currency. Being inside the top 20 cryptocurrencies in terms of market cap, Dash is a strong competitor to Tixl.

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 experience significant discussion or development until it caught the attention of crypto-world with Grin."[47] Grin is designed to be inflationary and the potential supply of Grin is infinite.[48]

Symbol:	GRIN
Form of organization:	Community-driven[49]
Launched:	January 15, 2019
Fees:	> $0[50]
Transaction speed:	> 1 Minute[51]
Ledger type:	Blockchain
Cryptosystem for signatures:	Elliptic curve secp256k1[52]
Cryptosystem for 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 obtain. The privacy guarantee of MimbleWimble, in this case, is equivalent to using Bitcoin and generating a new address for each new transaction (with the added advantage of hiding the TX amount)"[53]

[47] Mohamed Fouda | MimbleWimble: The Good and the Bad:
https://www.tokendaily.co/blog/mimblewimble-the-good-and-the-bad
[48] 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/
[49] Grin vs. BEAM, a Comparison:
https://tlu.tarilabs.com/protocols/grin-beam-comparison/MainReport.html
[50] Grin Economic Policy: Fees and Mining Reward:
https://github.com/mimblewimble/grin/wiki/fees-mining
[51] TM Lee | Grin: Frequently Asked Questions:
https://www.coingecko.com/buzz/grin-frequently-asked-questions
[52] Grin forum discussion: https://www.grin-forum.org/t/schnorr-signatures-in-grin-information/730
[53] Mohamed Fouda | MimbleWimble: The Good and the Bad:
https://www.tokendaily.co/blog/mimblewimble-the-good-and-the-bad

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 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.[54]

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 of Tixl in the longer term.

[54] Mimblewimble: the good and the bad: https://thebitcoin.pub/t/mimblewimble-the-good-and-the-bad/49971

2.9 Beam

Beam is another 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. These include an implementation of an auditable wallet and a feature that allows asynchronous negotiation of transactions. [55]

Symbol:	BEAM
Form of organization:	Beam Development Ltd.[56]
Launched:	January 3, 2019
Fees:	> $0
Transaction speed:	> 1 Minute[57]
Ledger type:	Blockchain
Cryptosystem for signatures:	Elliptic curve secp256k1[58]
Cryptosystem for encryption:	Elliptic curve secp256k1
Consensus algorithm:	Proof of Work (modified Equihash)[59]

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.[60]

Competition to Tixl

Although Beam, like Grin, can't compete with Zcash's privacy, Beam could become a serious competitor of Tixl over the longer term with the extensive feature list on the roadmap.

[55] Grin vs. BEAM, a Comparison: https://tlu.tarilabs.com/protocols/grin-beam-comparison/MainReport.html
[56] Beam FAQ: https://www.beam.mw/faq/what-is-beam-model-of-governance
[57] Beam FAQ: https://www.beam.mw/faq/what-is-the-block-time-and-block-size
[58] Beampedia: https://www.beam.mw/beampedia-item/elliptic-curve-cryptography
[59] 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
[60] Beam 2019 Roadmap: https://medium.com/beam-mw/mimblewimble-beam-roadmap-2019-b2c7f38fc106

2.10 Nano

Using its block-lattice structure, Nano aims 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. Firstly, each account on Nano's protocol has its own 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 is 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.[61]

Symbol:	NANO
Form of organization:	Nano Foundation (non-profit) and NanoLabs Inc.
Launched:	October 7, 2015
Fees:	$0
Transaction speed:	~15 Seconds [62]
Ledger type:	Block-lattice (DAG)
Cryptosystem for signatures:	Elliptic curve ed25519
Consensus algorithm:	Delegated Proof of Stake

Downsides

In 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 at the start, the transaction time has increased significantly. On Reddit, users report that transactions sometimes take more than 20 seconds. As a result, Nano has lost some of its reputation for super-fast transactions.

Nano seems unconcerned about it's lack of private transaction ability, and it is questionable whether Nano could even implement such a feature without significant changes.

Ongoing Improvements

According to the Nano roadmap, future work will focus on improving transaction speed and decentralization.[63]

[61] Colin Harper | What Is Nano?: https://coincentral.com/nano-beginners-guide/
[62] Reddit discussion: https://www.reddit.com/r/nanocurrency/comments/ald1et/nano_is_not_instant_at_least_not_literally
[63] Nano Roadmap: https://docs.nano.org/releases/upcoming-features/

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 focused on private transactions. Over the longer term, Nano is therefore not considered to be positioned as a direct competitor.

2.11 Tixl

Tixl uses the advantage of green field implementation and combines the best features of existing digital assets into one. As with Nano, Tixl uses a directed acyclic graph as its data structure, which supports instant transactions. To have a decentralized system that votes for validity of transactions quickly, Tixl uses the Stellar Consensus Protocol (SCP). Another huge advantage is that Tixl makes use of quantum secure cryptography, which is not used by any other competitor. The implementation of this feature helps future-proof Tixl.

Symbol:	TXL (MTXLT on exchanges)
Form of organization:	Tixl gGmbH (non-profit)
Launched:	not yet available
Fees:	$0
Transaction speed:	~0.5-10 Seconds (expected)
Ledger type:	Block-lattice (DAG)
Cryptosystem for signatures:	ECDSA (later XMSS)
Cryptosystem for encryption:	AES-256 & NTRU
Consensus algorithm:	Stellar Consensus Protocol (SCP)

Downsides

Whilst the timing of the development of Tixl 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 have the benefit of a head-start in terms of awareness, exchange listings, volume - and especially - well developed and supportive communities. While other digital assets are already in production, Tixl is still in development.

2.12 Final Thoughts

We have seen a lot of technological progress in the field of digital assets over recent years. For example, the quantum secure cryptosystem NTRU was released out of patent and developers all over the world can now use it. Alternative data structures and consensus algorithms have also proven themselves. This means there is more than that one simple blockchain now. There are also much greater advantages in a decentralized system to confirm a transaction is valid, as opposed to the relatively slow and power-consuming Proof of Work algorithm of Bitcoin.

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

3. Fundraising

Tixl makes use of token sales for fundraising. A token sale can also be called an ICO[64] which 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.

Legal disclaimer: For all information about fundraising, please also refer to the general terms and conditions.[65]

3.1 Why should a Token Sale be carried out?

The development of Tixl is laborious. A software development team is needed to implement the Tixl ledger in a step by step process. In addition, there are a number of associated aspects that need to be commissioned, these include social media, accounting, legal and tax services, as well as security audits.

Along with the combined developments costs, there is the (often large) cost to list on an exchange. Some exchanges may accept Tixl without a financial contribution, or in exchange for an amount in TXL itself. To be accepted as a cryptocurrency by the market, Tixl needs to be traded on major exchanges which frequently require payments of six-figure sums for listings.

The hosting of Tixl nodes should be decentralized over time. However, in the early days, 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 a number of marketing campaigns to achieve this. Here we face the same challenges as with exchange listings - for some marketing campaigns e.g., influencers or B2B partnerships, TXL may be issued, but others will require payments in USD, EUR or other Fiat currencies.

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

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

3.2 How is it possible to distribute Tixl Tokens during the Token Sale while Tixl is still undergoing development?

During the token sale, no actual TXL will be sold but Tixl tokens (TXLT) on an existing platform will be available for purchase. More precisely, they are launched as a BEP2[66] token with the short-code MTXLT (one million TXLT) on the Binance Chain[67]. To receive (M)TXLT a Binance Chain wallet[68] is required.

After completion of the technical development of TXL, the Tixl token holders will have the ability to swap their Tixl tokens (TXLT) for TXL at a ratio of 1 to 1. In other words, Tixl Token holders can swap their Binance Chain based MTXLT for TXL at a ratio of 1 to 1,000,000 (one million).

3.3 Can Tixl be traded now?

Tixl was listed on Binance DEX (Decentralized Exchange) on August 28, 2019. The MTXLT/BNB trading pair is available for trading on https://www.binance.org/en/trade/MTXLT-286_BNB. As at October 20, 2019, the price for one MTXLT was at 5.199 BNB or $95.00. The goal is to achieve more trading pairs on different (and also centralized) exchanges in the future.

3.4 Token Swap

The Tixl gGmbH will implement a bridge between the Tixl ledger (as soon as it is launched) and the Binance Chain. With that bridge it will be possible for a Tixl token owner to swap MTXLT BEP2 tokens to native MTXL and vice versa. A tutorial outlining the technical details, and requirements regarding the token swap, will be published on the Tixl website shortly after completion of the technical development.

Legal disclaimer: For more information about the token swap please refer to the general terms and conditions.[69]

[66] Binance Chain BEP2 Token Standard: https://github.com/binance-chain/BEPs/blob/master/BEP2.md
[67] Binance Chain: https://docs.binance.org
[68] Tixl Wallet Recommendation: https://medium.com/tixlcurrency/tixl-wallet-recommendation-31a1ab6b1927
[69] Tixl General Terms and Conditions: https://tixl.me/legal/general-terms-and-conditions

Fig. 1. Tixl MTXLT/BNB Trading Pair on Binance DEX

3.5 How many TXLT are sold for fundraising and what happens to the balance?

Figure 2 gives an overview of the TXLT distribution. It can be seen that the most substantial part (by far) is allocated to the token sale. The following list describes in detail the planned distribution of the balance of the TXLT.

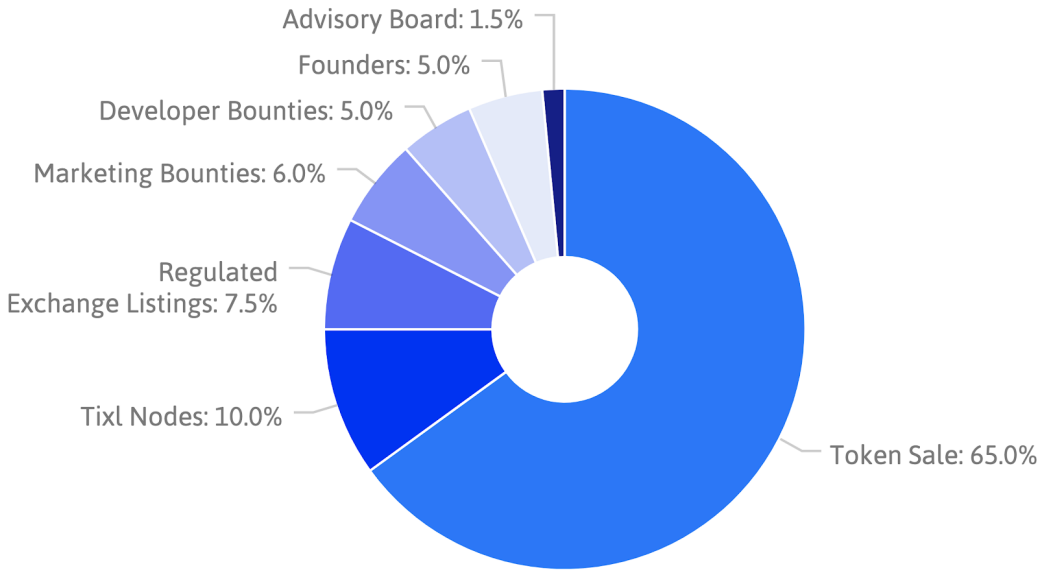

Fig. 2. TXLT distribution

Token Sale (65%): The most substantial amount of TXLT is allocated to the token sale.

Tixl Nodes (10%): The hosting of Tixl is associated with computing power that needs to be provided by someone. Chapter 5.5.4 discusses how TXL can be used as an incentive.

Regulated Exchange Listings (7.5%): Exchange listings are crucial to the distribution of a digital asset. With this additional provision, exchanges could be offered TXL to secure a listing.

Marketing Bounties (6%): With marketing bounties, the community or B2B partners have the opportunity to perform marketing services in return for TXL(T). For example, there is the option of providing an amount of TXL to payment providers integrating and promoting payments with TXL. Another example of a marketing bounty would be to let YouTubers explain the Tixl concept and receive TXL(T) in return.

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.

Founders (5%): The founders have financed the initial stages of the project and the preparations for fundraising. The most significant expenses included designs (logo, CI, documents), trademark application and legal advice. Therefore the founders shall have the ability to buy 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 will be a small payment in the form of TXL(T) for those advisors.

3.6 How will TXLT be offered?

Tixl fundraising started in Q2 2019 and is being conducted in different phases. Table 1 outlines the periods and the amount of tokens for sale. Starting at phase 3, tokens will also be sold privately to larger and strategic investors.

As Tixl was listed on exchanges before phase 3 began, the price determination must to be based upon the current market price. No private investor will purchase tokens from the Tixl gGmbH if they can buy cheaper on the open market. However, there are two instances where it makes sense for larger investors to purchase directly:

1. In the early days of the project the trading volume, and availability, of Tixl will be limited. As a result, investors may not be able to purchase a large number of tokens at the current market price. In this case, buying from the Tixl gGmbH would be a good option.

2. Larger, strategic investors are generally not interested in (day) trading Tixl tokens but will invest based on the envisioned longer-term success of the project. With this in mind, the plan is to sell tokens with holding periods, but at a cost just below the market price. As an example, assuming a market price of 50 USD per 1 MTXLT, it makes sense to sell 2,000 MTXLT to an investor from the payment industry for 25 USD per 1 MTXLT,

with a contracted holding period of three years. This benefits the project in two ways - firstly, MTXLT is in the hands of an investor who understands the long-term potential of a quality coin and secondly, those 2,000 MTXLT stay out of circulation for three years.

Phase	Period (Quarter / Year)	MTXLT for Sale
1	Q2 / 2019	22,500
2	Q3 / 2019	22,500
3	Q4 / 2019 - Q1 / 2020	10,000
4	Q2 / 2020 - Q3 / 2020	5,000
5	Q4 / 2020 - Q1 / 2021	5,000
6	Q2 / 2021 - Q3 / 2021	5,000
7	Q4 / 2021 - Q1 / 2022	5,000
8	Q2 / 2022 - Q3 / 2022	5,000
9	Q4 / 2022 - Q1 / 2023	5,000
10	Q2 / 2023 - Q3 / 2023	5,000
11	Q4 / 2023 - Q1 / 2024	5,000
12	Q2 / 2024 - Q3 / 2024	5,000
13	Q4 / 2024 - Q1 / 2025	5,000
14	Q2 / 2025 - Q3 / 2025	5,000
15	Q4 / 2025 - Q1 / 2026	5,000
16	Q2 / 2026 - Q3 / 2026	5,000
17	Q4 / 2026 - Q1 / 2027	5,000
18	Q2 / 2027 - Q3 / 2027	5,000
19	Q4 / 2027 - Q1 / 2028	5,000
20+	Q2 / 2028 - all tokens sold	5,000 each
	Total	**585,000**

Table 1. Tixl Fundraising Phases. The table shows the current planning and changes are possible (from phase 6 on the sales from the escrow will take place).

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

TXLT not sold in the token sales will be earmarked for later sale. These tokens will be split into 60 equal packages (as far as practicable) 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 comparable to how Ripple conducts its sales.[70]

[70] Escrow at Ripple: https://xrpl.org/escrow.html

3.8 Airdrop

To boost marketing, before and during the fundraising, a TXLT airdrop began on March 18, 2019 at 12:00 pm GMT. During this airdrop, 0.0005% of the overall TXLT supply - 4.5 MTXLT - were earmarked to be distributed free of charge. **Notice:** We initially started with an airdrop amount of 1% of the total token supply. Unfortunately, we realized that most participants in the airdrop did not add any benefit to the Tixl project. For this reason, we reduced the supply reserved for the airdrop. This decision was made by the Tixl team but was supported by a lot of investors from the Tixl community.

Every airdrop participant will receive 100 TXLT free of charge. The airdrop will end when the supply of 4.5 MTXLT is exhausted or the end-date of December 31, 2019 is reached. Any TXLT remaining at the conclusion of airdrop will be transferred into the escrow (see chapter 3.7).
On a date to be decided, but not before January 01, 2020, airdropped TXLT will be sent out on the Binance Chain. This is to avoid airdropped TXLT being sold during the first phases of the fundraising. An airdrop participant must store their public Binance Chain address on the Tixl account page until December 31, 2019 at 12:00 pm GMT. In the case where a participant does not provide a Binance Chain address, the associated airdropped tokens will be transferred into the escrow. The Tixl issuer address will be published on the Tixl website. A further requirement to confirm ownership of the Binance Chain account will be that the airdrop participant signs a message with their Binance Chain private key.

Before the airdrop token distribution, participants will be able to view the amount of TXLT to be received after January 01, 2020 on their account page. This number can differ from the actual amount of TXLT if the steps outlined in this section are not followed.

Legal disclaimer: As the tokens (TXLT) associated with the airdrop are distributed free of charge, participants do not have any legal entitlements, nor ability to make claims against the Tixl company, when receiving TXLT relating to participation in the airdrop. Please refer to the general terms and conditions.[71]

3.9 Airdrop Referral Program

There will be a referral program specific to 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 additional TXLT. As an example: 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

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

C = 100 TXLT
D = 100 TXLT

As seen above, 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 with 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 if the referred airdrop participant follows the steps from chapter 3.8 and provides an active Binance Chain account before 12:00 pm GMT, December 31, 2019. Until that time, the account page will display the total of the possible referral bonus in the event that all referred participants create active accounts. Please refer to the legal disclaimer in chapter 3.8.

3.10 Fund Utilization

The financial plans outlined below give an overview of the use of the capital collected from the fundraising. The following diagram describes how the money will be utilized. It should be noted that associated expenses do not necessarily apply during the same phase.

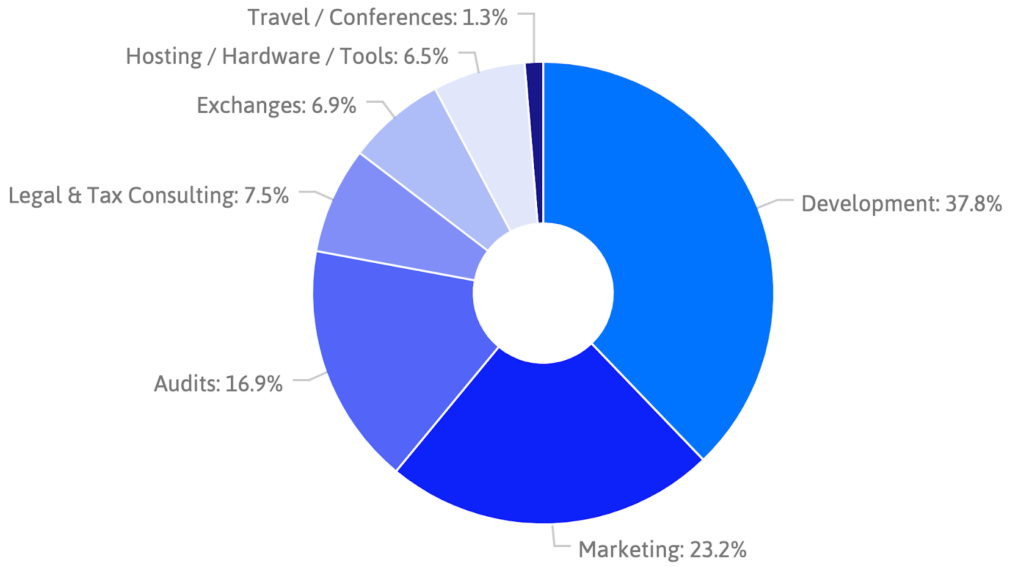

Fig. 3. Fund Utilization

The planned expenses have been categorized into distinct areas:

Product Development

Product Development encompasses all expenses related to the software development of Tixl. These mainly relate to the direct costs of personnel working on the development. Other related costs include - hardware, conception, and operation of a test network.

Marketing & Community

Equally as important as software development is the marketing of Tixl, and the maintenance and communication with the community. The planned budget is deliberately high to ensure the success of Tixl in the long term.

Security Audits

The security of the system is crucial. As a result, different forms of security audits and hacker attacks on a test network are planned during different phases.

Legal & Tax Consulting

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. There are also ongoing costs for accounting and tax consulting.

Exchanges

To ensure exposure to as many people as possible, listing on regulated exchanges is unavoidable. Widespread exposure also has a positive influence on Tixl's price. Accordingly, budget planning takes the costs of these listings into account.

Hosting & Hardware & Tools

For the operation of the test network and related, e.g. load tests, hosting costs will be incurred. There will also be other related expenses such as KYC provider fees and software tools.

Travel & Conferences

Especially during the early stages of the project, it's important to present Tixl at appropriate conferences and related events. Travel costs are incurred and speaker slots sometimes have to be purchased. We assume that the costs of speaking time should decrease as awareness of the project grows, and organizers may even subsidize travel costs entirely. For these reasons we have budgeted for travel and conference expenses to decrease in the later phases.

3.11 Investment Potential

Legal disclaimer: There is no guarantee that MTXLT (or later, MTXL) will increase in value. At this point, we would like to draw attention to the investment risks outlined in chapter 7. With any new venture, no matter how large or small, there are associated investment risks. It should be noted that the following returns in no way purport to be guaranteed, nor do they commit Tixl gGmbH to achieving these results. The calculations used are simply a way of forecasting potential returns (based on combinations of variables), that may help investors work out the possible return on their investment. We encourage every investor to make their own calculations, based on variables personal to them, and would stress that you should never invest more than you can afford to lose.

Table 2 shows various ways in which an investment in Tixl could develop. Each scenario outlines a potential return 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:

$$MTXLT\,Market\,Cap\,(USD) = Circulating\,Supply * Price\,per\,MTXLT\,(USD)$$ [72]

For the investment cases in Table 2, a circulating supply of 270,000 MTXLT is assumed, representing 30.00% of the total supply (900,000 MTXLT). Tokens can be considered in circulation if they are available for trades on the public markets. That means they:

- do not belong to the Tixl gGmbH.
- are not covered by lockup periods which would prevent them from being sold on the public market.

The circulating supply can change at any time depending on sales, bounty campaigns or other token distributions and should be considered as an example only.

The investment cases in Table 2 refer to a market capitalization of $1,000,000,000. This corresponds approximately to the market capitalization of Monero during September 2019[73]. If the price per MTXLT in USD with a market cap of $1,000,000,000 is to be determined, the following calculation applies:

$$Price\,per\,MTXLT\,(USD) = \frac{\$1{,}000{,}000{,}000}{270{,}000\,MTXLT} = \$3{,}703.70$$

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:

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

[72] The circulating supply is the quantity of a currency in circulation.
[73] Monero Market Capitalization: https://coinmarketcap.com/currencies/monero/

The goal is to achieve a higher market capitalization with Tixl, meaning the figures in Table 2 would have the potential to increase.

Case No.	Price per MTXLT	Amount of MTXLT Purchased	Total Purchased Value	Value at One Billion$ Market Cap	ROI
1	$20	10	$200	$37,037	∼185x
2		100	$2,000	$370,370	
3		1000	$20,000	$3,703,700	
4	$100	5	$500	$18,519	∼37x
5		50	$5,000	$185,190	
6		500	$50,000	$1,851,900	

Table 2. Investment Potential

4. Organizational Form

4.1 Team

The Tixl team consists of eight core members. Tixl is a company of the elbstack GmbH, meaning the Tixl gGmbH can utilise the services of the elbstack GmbH, when needed. In the past, various team members of elbstack have assisted Tixl with feedback, code reviews and design improvements. The following is a brief overview of the individual team members.

Christian Eichinger
Managing Director

- M.Sc. Software Engineering Leadership
- Founded elbstack in 2015 and expanded the company to 20 employees in 2019, with the company remaining profitable at all times
- Expert in translating mathematically defined cryptography to source code

Sebastian Gronewold
Managing Director

- M.Sc. Software Engineering Leadership
- Founded elbstack in 2015 and expanded the company to 20 employees in 2019, with the company remaining profitable at all times
- Started to study alternative consensus algorithms early in 2017 when Proof of Work was still state of the art

Bernd Strehl
Head of Development

- M.Sc. Information Systems
- 10 years of programming experience
- Specialized in algorithm development

Christopher Obereder
Chief Marketing Officer (CMO)

- 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

Mike Lohmann
Technology Consultant

- Founded elbstack in 2015 and expanded the company to 20 employees in 2019, with the company remaining profitable at all times
- Has in-depth knowledge, and years of experience, in setting up complex software architectures that can scale up to millions of users
- Helped many companies stress-test their environments before launching large-scale marketing campaigns

Leon Szeli
Chief Evangelist

- M.Sc. Consumer Affairs: Technology Innovation
- Researcher at Stanford University
- Researcher at University of Cambridge
- Entrepreneur building human-centered digital products

Vihren Stoev
Cryptographer

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

Lennart Brandt
UX and Digital Product Designer

- B.Sc. Information Systems
- Joined elbstack in 2016
- Has built complex UIs for several companies across Germany

4.2 Business Model

Due to the fact Tixl has no transactions fees it is hard to find a classic business model to compare it with.

Initially, the organization behind Tixl will be funded by issuing TXLT through token sales and later by potentially selling TXL from the escrow.

The founders are dedicated to the long-term performance of Tixl and are therefore heavily invested in its success. Due to this fact, their remuneration/investment is wholly by way of holdings in Tixl. All of the Tixl owned by the founders will have a lock-up period of 24 months, with the TXLT tokens later being swapped to TXL. At the conclusion of the lock-up period these TXL will be released for potential sale in installments from June 2021. After this date, the founders will be limited to selling just 1% of their tokens each month. The final 1% will be unlocked in September 2029.

4.3 Legal Form

When choosing a suitable legal form, a number aspects were taken into consideration. The most important criteria were ensuring the 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 in the future is conceivable, but not mandatory.

Further to this, a German non-profit company was chosen to ensure that that Tixl is recognized as a fully legitimate project. A more detailed explanation for choosing this company form can be found on the Tixl Medium blog[74].

[74] Efforts to protect Tixl investors:
https://medium.com/tixlcurrency/efforts-to-protect-tixl-investors-7daef7340014

4.4 Trademark and Patent Rights

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

There are currently no patent registrations. However, patent filings are not ruled out in the future. The basis for a patent could be, for example, specific concepts in cryptography that distinguish Tixl from established digital assets. Importantly for Tixl investors, patents provide protection as they prevent cloning of the Tixl system.

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

5. Technical Solution

The technical solution is one of the determining factors providing superiority over other existing digital assets. A combination of different approaches puts Tixl in this position. The most important components are Tixl's data structure, the applied cryptosystem, a sophisticated privacy concept and its chosen consensus algorithm.

5.1 General overview

Following, we will present the concepts of Tixl. First in a general and then comprehensive way and in the following sub-chapters the building blocks are described in more detail.

5.1.1 Data Structure

Tixl uses a *Directed Acyclic Graph* (DAG). Each account has an *accountchain* and multiple *stealthchains*. The *accountchain* contains an initial *account* block and multiple *open* blocks. The *account* block provides the identity of the account as it contains the public keys, that are necessary to send transactions to the account. The *open* blocks contain the access to the *stealthchains*.

Stealthchains will be created for each correspondence with another account. For example, if user A wants to receive funds from user B, user A creates a *stealthchain* BA. *Stealthchains* can only contain *open* and *receive* blocks besides the initial *open* block. To receive funds, a *receive* block that references a *send* block is created. These funds can be spent or transferred to another *stealthchain* by issuing a *send* block.

More information about the data structure in chapter 5.2.

5.1.2 Privacy Design

The account is opened by creating an accountchain. The first block on the accountchain is the "account" block and contains a NTRU key pair and a signature key pair. The private keys are encrypted with AES-256 and are also stored on the "open" block. The 256-bit AES key is the access to the account, it is short enough to be in compliance with BIP39[75]. Using the NTRU private key as the secret that accesses the account is a problem because of the huge key size and thus is not BIP39 compatible. AES-256 encrypted ciphertexts are shorter than NTRU encrypted ciphertexts. A 256-bit AES key requires a seed phrase of 24 words.

[75] BIP39 spec: https://github.com/bitcoin/bips/blob/master/bip-0039.mediawiki

The keys needed for the access of the generated stealthchains will each be stored on a block of the accountchain. The access to these chains will be also be encrypted with AES-256.

Amounts and balances on "send" and "receive" blocks will be encrypted with AES-256 for the issuer of the block and with NTRU for the receiver of the block. The blinding factors for the zero-knowledge proofs will be encrypted with NTRU. The amount and balance will be verifiable for third parties by the use of pedersen commitments and range proofs. Ownership over the account - or stealthchain - will be proven by the signing of the blocks with the chain's private signature key, which is individual for each chain.

The aforementioned mechanisms will ensure private transactions. However, with only these measures in place, it is still possible to infer relations between different stealthchains with additional information that may be obtained by being a part of multiple transactions. For example, a big retailer that uses Tixl as a payment method could link the stealthchains of two persons for which it knows the identity - stealthchain pair - to their employer, if the employer also makes payments to the retailer and pays out the employees in Tixl. To break this traceability Tixl will implement cut-through transactions by using *ValueShuffle*.

More information about the crypto systems in chapter 5.3 and information about cut-through transactions can be found in 5.4.

5.1.3 Validators

The most important piece of the architecture are the validator nodes or *validators*. They store the transactions in instances of the ledger, validate transactions, and determine the global state of the Tixl ledger using the Stellar Consensus Protocol (SCP). All running instances of *validators* will be called the validator network.

A transaction that, for example, is generated by the wallet software, is sent to the *gateway* and the gateway broadcasts this transaction to all known *validator nodes*. If the transaction is valid, all validators should vote to include it in the next *slot*[76]. Invalid transactions should be rejected by all correct validators. If one validator is approving invalid transactions, regardless of this happening out of malicious intent or due to a program error, the whole network should still reject the transaction because no quorum for the invalid transaction is reached.

SCP makes use of a concept called *quorum slices*. Each validator that runs SCP, which can be any person or organisation, can define which sets of other validators it deems sufficient to be convinced by a statement. This implicitly leads to a ranking of trust in validators. Validators that are run by trustful organisations and don't vote for invalid transactions will gain trust, over time, by being included in the *quorum slices* of evermore other *validators*. Opposingly, those validators that vote for invalid transactions will be considered untrustworthy.

More information about the consensus in chapter 5.5 and about the architecture in chapter 5.6.

[76] A slot is defined as a round of the consensus protocol.

5.1.4 Transaction lifecycle

Assuming A wants to send 10 Tixl to B, the full lifecycle from creation to network acceptance would look as follows:

A already has a *stealthchain* with 10 or more Tixl as a balance (or more than one *stealthchains* with 10 or more Tixl in total). A uses the id of the *accountchain* of B as an address for the transaction. The wallet software will look up the necessary keys to create the transaction containing the *send* block. Specifically, the NTRU public key is used to encrypt the amount, and blinding factor, for B.

The wallet software sends the transaction to the *gateway* and the *gateway* forwards it to the *validators*. The *validators* work to validate the transaction each against their own ledger. The transaction should be recognized as valid by all honest validators, and the validators will include it in the next slot of the consensus protocol.

As the send transaction is confirmed by the validator network, B scans the *send* blocks and tries to calculate a feasible transaction amount by decrypting the blinding factor and amount with its private NTRU key. If a feasible amount is found, the transaction is addressed to B and B will create a *receive* block and send it to the gateway.

The transaction containing the *receive* block is processed in the same way by the network. If the *validator network* confirms the transaction it can be seen as complete.

Every account that knows the blinding factor can claim the *send* block with a *receive* block. In general, those are the accounts that own the private NTRU key to decrypt the blinding factor, and also the sender itself. A transaction should only be deemed as complete by the receiver when its *receive* block is confirmed by the *validator network* as that sender could also reclaim the block. This mechanism also allows the ability to restore the transaction, when a wrong address has been used.

Instant transactions are also possible as peer to peer transactions, if both parties trust each other.

More information about transaction in chapter 5.4

5.2 Data Structure

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

5.2.1 Which Data Structure does Tixl use to Persist Transactions?

The Tixl ledger is a special implementation of a *Directed Acyclic Graph* (DAG)[77]. The implementation of Tixl is similar to the *block-lattice*[78] 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 may even have multiple blockchains per user depending on the number of transaction partners.

5.2.2 Block Structure

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

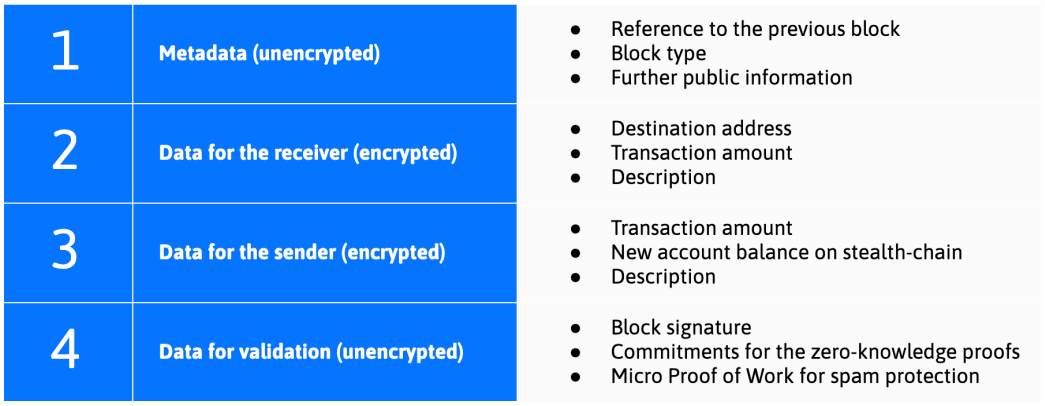

Fig. 4. Block Structure

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)
Information that the recipient should get without anyone else on the network being able to read it. That includes the amount of the transaction and an optional description.

[77] 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/
[78] Block Lattice: https://docs.nano.org/integration-guides/the-basics/#block-lattice-design

Data for the sender (encrypted)

The sender would also like to be able to view the amount they have sent. Therefore, the sender encrypts specific data for themselves. In addition to the amount, this also affects the balance on the stealthchain. In the case where 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, for both the sender and the recipient, produces duplicate data. This overhead will be accepted in favor of privacy.

5.2.3 How much Memory is Needed per Tixl Transaction?

For a Tixl transaction, multiple blocks are generated and, due to the cryptographic requirements, Tixl transactions are expected to consume more storage space. Currently, the required storage space of a block cannot be quantified exactly, but we expect a size of 7.000 to 9.000 bytes for send and receive blocks.

5.2.4 Scalability

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

5.2.5 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.

Transaction speed can generally be traded for trust, this results in multiple theoretical levels of transaction speed and trust:

- Peer to peer transaction **(High Trust - Instant Transaction)**: A transaction can be directly sent from peer to peer and the receiver validates the transaction and accepts it. The acceptance of the transaction happens asynchronously to the sending of the transaction to the validator network. This peer to peer transaction type is especially suited for payments without direct exchanges of real world goods, for example a friend paying back the money for lunch he/she laid out. Estimated speed: $<$ **500ms**.
- Single stop validation **(Medium Trust - High Speed Transaction)**: The sender can send a transaction to a single validator and the receiver confirms the transaction, when the validator deems the transaction valid, before it is confirmed by the full validator network. This method is relatively secure especially when the validator is highly trusted by the receiver. A good usage scenario is a point of sale transaction of a retailer. The retailer could run its own validator and the payer sends the transaction to that validator, if it's considered valid by the validator of the retailer the transaction is done. Estimated speed: $<$ **1s**.
- Full validation **(No Trust - Medium Speed Transaction[79])**: The transaction is sent to the validator network and is only accepted when the validator network confirms the transaction. When the transaction is confirmed by the validator network it can not be revoked, so there is no need for trust between the payer and the payee. This is the standard mode of any transaction and should be used in most cases. Estimated speed: **5 - 10s**.

5.3 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 digital asset 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 anyone 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 has existed for a long time, but in recent years some of the tech giants have started to make practical progress toward making them a reality. And whilst the advent of a practical, usable, functioning, well-programmed quantum computer may be some way off, the potential for their implementation already factors in the minds of the cryptographic community. As always, people's ideas far proceed their practical implementation, and years before anything related to quantum computers started to become a reality, Peter Shor invented

[79] The speed is still high compared to most cryptocurrencies, e.g. Bitcoin 10-60+ min.

an algorithm (correspondingly named Shor's algorithm), which uses the theoretical power of a quantum computer to solve the factorization problem (if you have a number, finding 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 can also be solved, theoretically, using Shor's algorithm. Almost all digital signatures are not secure anymore. And now, as quantum computers are gradually becoming a reality – the world needs to change. It doesn't matter if the practical implementation of quantum computers is achieved within the next 10 years (in line with the most hopeful predictions), or over the next 15-20 years (a more realistic time-frame), nor does it matter greatly that any change will come slowly, or even that a working, state of the art quantum computer will still take considerable time to decode any particular data - the fact remains that anyone who wants to stay ahead of these 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 retains its strength in the face of quantum computing.

5.3.1 Cryptography and Quantum Security in Tixl

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

Since the Tixl prototype is still being developed, a final decision regarding the cryptosystem to be utilized cannot be made yet. However, ECDSA, which will later be changed to *XMSS*, is being considered for the signature section and, for the encryption part, *NTRU* seems to be a good fit.

5.3.2 Encryption

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 concerns that, for smaller N (degree of the polynomial), some attacks were effective. With the potential advent of quantum computing, NTRU drew renewed attention and the different forms of attack were studied in greater detail. Greater scrutiny of the possible values of the parameters proved certain rings to be weaker and

others to be more robust, and provably secure versions were created as early as 2013.In 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.[80]

AES

The Advanced Encryption Standard (AES) is a symmetric encryption scheme, which means that the same key is used for encryption and decryption. Due to its nature, it can't be used to share information between parties on the blockchain (except with a key exchange). AES comes with 3 different security levels: 128, 192 or 256 bits. Tixl will use AES-256, because it is the most secure. Quantum computers will reduce the effective security to 128-bit, which is still sufficient. We can use AES-256 to encrypt things that need to be private and only accessed by the writer, for example the keys for stealthchains or the amount and balance. Note that the amount and balance will also be encrypted with NTRU for the recipient of the transaction. Also, because the keys for NTRU are very large (4411 bits key size for 128-bit security), a seed phrase to create such a key would be huge and not conform to BIP39, so the NTRU private key would be stored on the accountchain encrypted with AES-256, with the AES-256 secret key allowing access to the account (and created by a mnemonic seed phrase).

5.3.3 Signatures

Signatures are necessary to prove the ownership of the accountchains, stealthchains and blocks. The owner that has access to the private key creates a signature that is publicly verifiable by the validators or other third parties, thus allowing only the owners to write blocks on their chains and to create new chains. With the launch of Tixl we will use *ECDSA* for signatures and later switch to a quantum resistant system, as it becomes necessary.

ECDSA

The Elliptic Curve Digital Signature Algorithm with the Secp256k1 curve became popular through its use by Bitcoin[81]. Elliptic curve cryptography is known for providing good security in relation to key-size compared to its alternatives - like RSA. However, since the security of this crypto-system is based on the elliptic-curve discrete-logarithm problem, it is also vulnerable to Shor's Algorithm, which means that it is not quantum resistant.

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

[80] NIST | Post-Quantum Cryptography: https://csrc.nist.gov/Projects/Post-Quantum-Cryptography/Round-2-Submissions
[81] Bitcoin Wiki: https://en.bitcoin.it/wiki/Secp256k1

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 discover a solution to that problem which would compromise the security of the signatures. It is quantum secure and no developments in quantum computing 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 also makes XMSS forward-secure, which means that even if a secret key is compromised, all previous signatures remain valid and are not compromised.

Note on transition of ECDSA to a quantum secure signature: We do not see the lack of quantum resistance as a problem for now because we can upgrade the keys of the chains later, when the threat to ECDSA due to quantum computers becomes more imminent. In addition, the usage of ECDSA will, for now, allow us to keep the block size a little smaller. If we reach this threshold in the cryptograhic ecosystem, the validators will be required to only accept transactions that are signed with a new quantum secure signature. Before that, there will be a period where chains will be required to announce a new, quantum-secure, signature key and sign it with their old signature key. We will ensure that there is enough time before the validators stop accepting the old keys and that the official wallet software will do it automatically. However a failure to upgrade the key could result in the loss of funds.

5.4 Private Transactions

Tixl achieves private transactions by combining different approaches. First of all, a TXL owner will be protected so that nobody can see their balance. To achieve this, TXL are not written to the personal blockchain (*accountchain*) of a user but instead to unclassifiable blockchains (stealthchains) only known by recipient and sender. Correspondingly, a TXL sender must also be protected so that their outgoing transactions cannot be seen. Tixl achieves this by sending TXL directly from stealthchains that a new recipient cannot relate to other TXL owners.

The section about confidential transactions explains how it is possible for the amount of a transaction, as well as account balances, to remain *invisible* to anyone but the owner whilst still making it possible to be processed and validated by a decentralized consensus algorithm.

5.4.1 Accountchain

The accountchain represents the user's main account. It is used to store encrypted references to the user's stealthchains.

5.4.2 Stealthchain

A stealthchain is a separate blockchain that works much like a Monero stealth address[82]. For each sender/receiver combination, the first transaction generates a new stealthchain. Other blocks of the same sender are written to the same stealthchain by the receiver.

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

5.4.3 Confidential Transactions

The goal of confidential transactions[83] 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.

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.[84]

[82] Monero Stealth Address: https://getmonero.org/resources/moneropedia/stealthaddress.html
[83] Adam Gibson | An investigation into Confidential Transactions: https://github.com/AdamISZ/ConfidentialTransactionsDoc/blob/master/essayonCT.pdf
[84] Beampedia | Zero-knowledge Proof: https://www.beam.mw/beampedia-item/zero-knowledge-proof

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.[85]

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.

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.

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.

$C(BF_1, number_1) + C(BF_2, number_2) = C(BF_1 + BF_2, number_1 + number_2)$[86]

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.

[85] Tommy Koens et. al. | Efficient Zero-Knowledge Range Proofs in Ethereum: https://www.ingwb.com/media/2667860/zero-knowledge-range-proofs.pdf

[86] Pedersen Commitment: https://www.beam.mw/beampedia-item/pedersen-commitment

5.4.4 Private Transactions Visualized

In this chapter, the technical infrastructure of Tixl is explained in detail regarding the interaction of its different components (DAG, accountchain, stealthchains, encryption, signatures, etc.). Tixl is using a DAG as the underlying data structure. The accountchain and stealthchains 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 5 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.

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

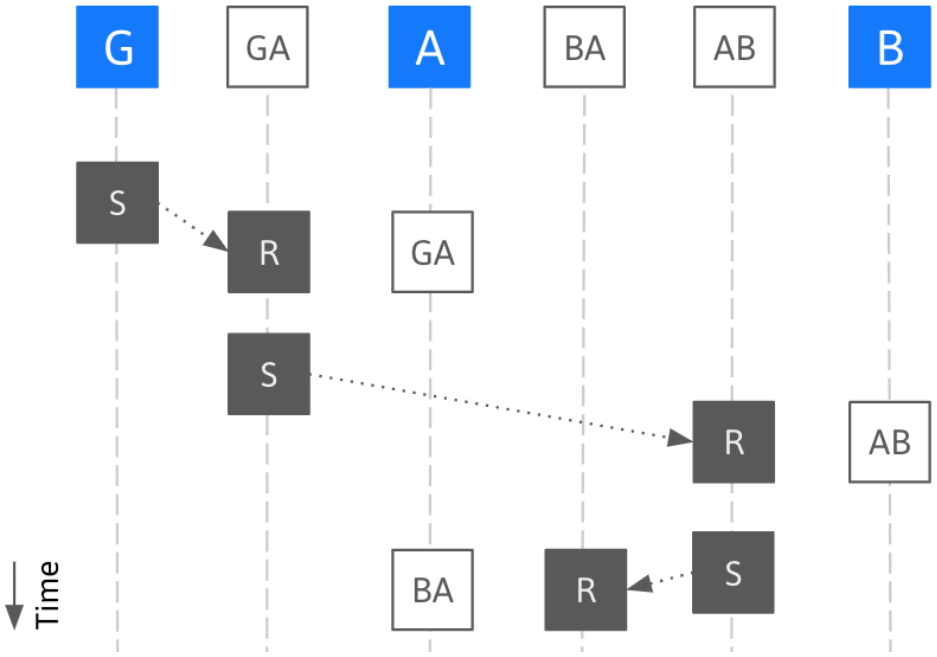

Fig. 5. Tixl DAG with accountchains (G, A, B) and stealthchains (GA, BA, AB)

A stealthchain cannot be assigned to an accountchain by an outsider. Since the transactions are received on stealthchains and the amounts are never transferred to an accountchain, the recipient is completely protected. Since the receiver is protected, the sender is also protected because the send block is also saved on the stealthchain. Only the Genesis account can be

identified as the sender, because it does not send from a stealthchain. That is not a problem, and even desirable.

To ensure that only an owner can write a new block on their chain, blocks are verified by signatures. Tixl considers the use of ECDSA for signatures first and will upgrade to XMSS in the future, to be prepared for the advent of quantum computers.

Tixl aims to provide the highest level of privacy. Therefore, it is crucial that the amounts and balances are encrypted before they are sent to the network. For amount and balance encryption, NTRU will be used. NTRU is known for its speed and efficiency and has been used in business applications 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 by using *ValueShuffle*[87], an extension of *CoinShuffle++*[88]. ValueShuffle is a decentralized protocol, which will be run with the participants wishing to mix their coins and results in a multi-transaction with multiple inputs and outputs, which are unlinkable. We can leverage the concept of quorum slices of the Stellar Consensus Protocol to select the nodes that are most trusted that will function as a bulletin board for the protocol. The downside of this method is that constructing such a multi-transaction consumes extra time. However, we don't see this as a big problem because the main purpose will be to use *ValueShuffle* to move funds to fresh stealthchains and not to use it directly for transactions between two parties. The wallet software could do this automatically in the background so that it doesn't become time critical. Quantum security for this protocol is not yet a priority because, even if the used addresses became linkable after breaking the non-quantum crypto systems, the funds could be moved to new stealthchains with an updated protocol version at any stage.

5.4.5 Scalability

Since encryption and decryption take time, it's important to keep the performance of the utilized algorithms in mind when building a digital asset that needs to scale up to thousands of transactions per second. As soon as the Tixl prototype reaches a state which allows the measurement of times for encryption, signing, decryption, and validation, this whitepaper may be updated with more information about those impacts on Tixl's scalability.

Also, consideration must be given to the fact that there are new stealthchains for every sender/receiver combination. Currently, if a Tixl user wants to send a larger amount of TXL and needs to merge funds of several stealthchains, this would multiply the regular encryption time per block by the number of stealthchains. Looking at different solutions, an easy way of solving this in the beginning could be to have a clean-up feature implemented by wallets. Wallets would transfer and merge funds to a single stealthchain when idling.

[87] ValueShuffle Paper: https://people.mmci.uni-saarland.de/~truffing/papers/valueshuffle.pdf
[88] CoinShuffle++ Paper: https://crypsys.mmci.uni-saarland.de/projects/FastDC/paper.pdf

5.5 Consensus

The Tixl consensus algorithm holds decentralized voting on transactions to always make sure only valid transaction are included and all participants of the consensus algorithm will confirm the same transactions.

5.5.1 What are Tixl Nodes and the Tixl Network?

A *Tixl node*, *validator node* or short *validator* 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* or *validator network*.

Nodes are needed to perform transactions in general. They save the history of all Tixl transactions in the ledger and thus make payments possible. Otherwise, transactions would only be stored on the sender and receiver devices and would be lost if these devices were lost.

An additional essential task of the nodes is the validation of transactions. A transaction may only be written into the global transaction ledger if it is valid. A transaction may be invalid due to software errors (e.g. in a Tixl app.) or sent by malicious users in the network. In this case, the transaction will be rejected by the validator network.

5.5.2 How do Tixl Nodes Reach Consensus?

Many of the existing consensus algorithms, like *Proof of Work* (PoW)[89] or *Proof of Stake* (PoS)[90], 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."[91] An explanation is given in the following sub-chapters starting with the root issue, the Byzantine generals problem, as a result of which SCP was created.

[89] Binance | Proof of Work (PoW) Consensus Algorithm:
https://www.binance.vision/blockchain/proof-of-work-explained
[90] Binance | Proof of Stake (PoS) Consensus Algorithm:
https://www.binance.vision/blockchain/proof-of-stake-explained
[91] Bob Glickstein | Understanding the Stellar Consensus Protocol:
https://medium.com/interstellar/understanding-the-stellar-consensus-protocol-423409aad32e

The Byzantine Generals Problem & Byzantine Agreement

The name of the Byzantine generals problem comes from a paper[92] from 1982, written by Leslie Lamport. Together with two co-authors, Lamport described the following allegory for the problem of decentralized decision making: The night before a possible battle, a group of Byzantine generals tried to decide whether to attack together or retreat. Messengers exchange the messages between the generals. Now there is a problem: Some of the generals, and also the 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*.

Federated Byzantine Agreement (FBA)

Federated Byzantine agreement (FBA) expands traditional Byzantine Agreement by open membership, meaning that the participants can change. 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 FBA is to defeat those attacks by introducing *decentralized quorum selections*. SCP is a certain kind of FBA system.

Stellar Consensus Protocol (SCP)

David Mazières introduced SCP in a whitepaper[93] in 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*.

Each node v selects it's own quorum slices $S(v)$, which are sets of other nodes. Each of these sets is sufficient to convince v of a statement, if all nodes of the slice agree. A quorum slice must also contain the node v itself. 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

[92] Leslie Lamport et. al. | The Byzantine Generals Problem: https://people.eecs.berkeley.edu/~luca/cs174/byzantine.pdf

[93] David Mazières | The Stellar Consensus Protocol: A Federated Model for Internet-level Consensus: https://www.stellar.org/papers/stellar-consensus-protocol.pdf

collectively speaks for the whole network."[94]

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 n_1, n_2, n_3, n_4 have the following quorum slices S:

$S(n_1) = \{\{n_1, n_2, n_3\}\}$
$S(n_2) = \{\{n_2, n_3, n_4\}\}$
$S(n_3) = \{\{n_2, n_3, n_4\}\}$
$S(n_4) = \{\{n_2, n_3, n_4\}\}$

Note, that this is a set of sets, which means that each node can have multiple quorum slices.

In this case $\{n_2, n3, n4\}$ would form a quorum because it contains a quorum slice for each of its members. If a quorum also containing n_1 should be formed, this would have to include all nodes $\{n1, n2, n3, n4\}$, because n_2 and n_3 will not agree on a statement without n_4 agreeing as well.

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 agreement on whether this transaction will be included or not. Now, a node receiving the transaction, that was elected as a leader for the *slot*[95], begins by casting a *vote* for the transaction to be included. 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 to all accept it and can then *confirm* the outcome.

There are situations that can arise where 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 SCP whitepaper. Furthermore, the Tixl consensus algorithm, based on SCP, will be made available open source, so code examples for handling such cases will follow.

5.5.3 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 pruned history that contains only the necessary information to validate transactions (*light node*).

The reason for having two different types of nodes lies in the massive storage requirements as the number of transactions increase. For example, if the consumption for one transaction were 1 kilobyte, the entire ledger would be 100 gigabytes with 100 million transactions.

[94] David Mazières | The Stellar Consensus Protocol (SCP): https://tools.ietf.org/html/draft-mazieres-dinrg-scp-03
[95] A slot is one round of the consensus algorithm.

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

5.5.4 What is the Tixl Node Incentive Program?

It is safe to assume that in the early phase of the project the motivation to host an 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 longer term, Tixl will employ a similar approach to Ripple. It should create intrinsic motivation for larger TXL owners to secure their assets by hosting an historical node, as this contributes to the stability of the Tixl network.

5.5.5 Will Tixl be 100% Decentralized from the Start?

Tixl's primary focus is on usability, widespread usage and protection of investors. To achieve these goals the system does not have to be completely decentralized from the very beginning. In no way do we want to diminish the importance of decentralization with this approach. However, achieving key goals is more crucial to the project than decentralizing right from the initial launch. It remains one of Tixl's top priorities to become a 100% decentralized digital asset as soon as possible.

5.5.6 Scalability

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.[96]

5.6 Architecture

This chapter describes the general architecture and how the different modules are orchestrated. Note, that the architecture is mainly designed for the prototype so far, some aspects may be changed later during the development of the actual Tixl network.

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

5.6.1 Overview

Figure 6 provides a general overview of the architecture and shows how the different components - explorer, wallet, gateway, validator node and witness node - communicate.

Validator Node

The validator nodes are also called Tixl nodes and provide the essential functionality of the Tixl network. In the next section the architecture of the validator nodes are described in more detail. All validator nodes communicate with each other in the validator network. Ideally the validator nodes will use a broadcast to communicate their information to all the other nodes. There is no confidential information communicated in this network, so it is desirable that anyone can join and listen to messages sent. The basic function of the validator nodes is to validate transactions, find a consensus with all other nodes on which transactions to include and then store those in the ledger.

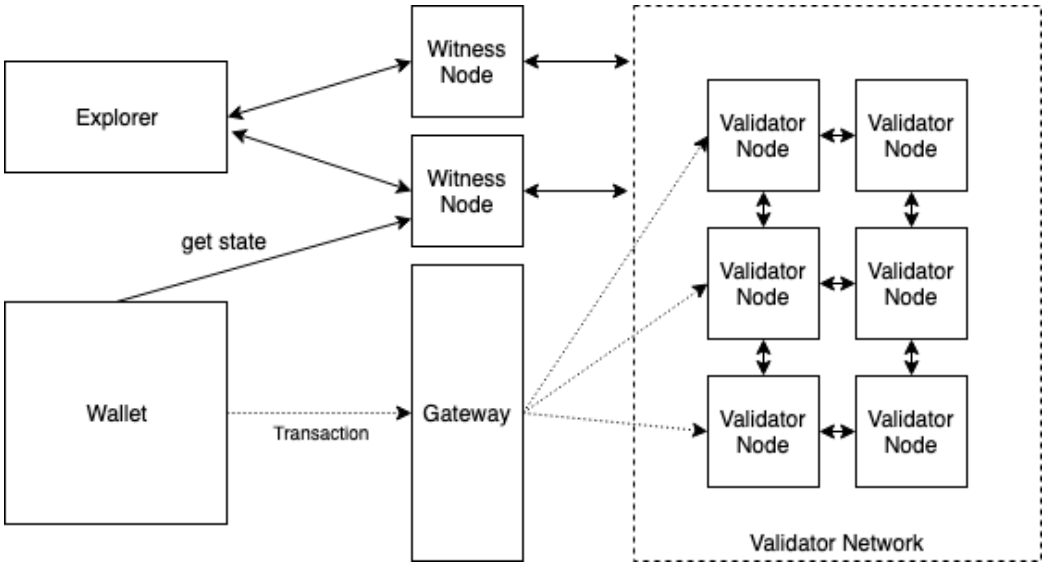

Fig. 6. General architectural overview

Gateway

Transactions need to be sent to at least one validator to be processed by the network, but sending transactions to only one validator will lead to long processing times because each validator is only eligible with a certain probability to propose transactions to the network. The gateway basically provides a similar HTTP-Interface as the validators, and also accepts transactions. Validators can register at the gateway and will receive incoming transactions from the gateway, this results in a distribution of transactions to the validator network, hence, wallets and other components that issue transactions should send transactions to a gateway, and not directly to validator nodes. Possibly later, the gateway should be replaced by a layer for the validator nodes

that distributes transactions through the validator network, so that transactions can be send to validator nodes directly, for more decentralization.

Witness Node

Witness nodes are similar to validator nodes, but instead of actively participating in the consensus they just listen to externalized transactions and store them. They can be used by other components to get the state of the network, e.g. get the latest transactions or subscribe to transactions. This functionality could also be included in the validator nodes but this would introduce even more network traffic and processing to them and it is better to reserve those capacities for participation in the consensus.

Wallet

The wallet component could be a native mobile wallet or a web wallet. It's main purpose is the display of transactions for a certain user and the issuing of transactions for that user. Transactions will be sent to the gateway and the state will be obtained from witness nodes.

Explorer

The explorer shows the latest transactions and slots with additional information. The information gain is limited because transactions are private and thus there is not much to learn from them but the amount of processed transactions could be seen here.

5.6.2 Validator Nodes

A validator node, or validator, consists of three main components: consensus, ledger and an intermediate storage, it also has two interfaces: one exposes a HTTP API and the other is reserved for communication with other validators. When the validator receives a transaction via the HTTP API (most likely from the gateway), the following steps will occur:

- The micro proof of work of the transaction will be validated. If the micro proof of work is invalid, the request will fail immediately.
- If the micro proof of work is valid, the transaction will be stored until the next slot of the consensus begins.
- When the new slot of the consensus begins, and the transactions from the slot before have been written to the ledger, the transactions are sent to the ledger for validation. The ledger does an in-memory fork of the state for the current slot to validate all transactions successively. With usage of the crypto component, the signature and range proofs are validated, to make sure that the transaction is valid in terms of authenticity and balance.

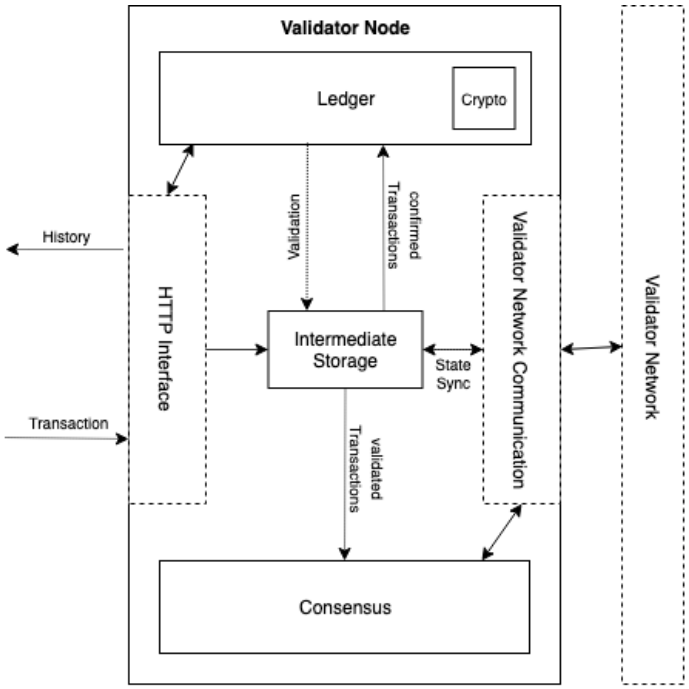

Fig. 7. Anatomy of a validator node

- Invalid transactions will be discarded and valid transactions will be stored until the consensus requires the information of validity. In the case that the validator becomes a consensus leader for the slot, it will propose all valid transactions to the network. When the consensus receives a vote for transactions it will also vote for those that it considers valid.
- At the end of the consensus slot a list of transactions will be externalized. Those are forwarded to the ledger module to be persisted.

Validator state

When a node starts initially or looses synchronization, for example by missing messages from the consensus, because of an unreliable network, it will set it's state to *synchronizing*. In the synchronizing state the node will reach out to one of its peers to request the transactions that it missed. Whenever a transaction is stored, a master hash is calculated that depends on the prior master hash and the new transaction. Upon receiving all transactions, the node requests the master hash from its other peers and compares that hash to its own calculated master hash to determine if the node received all of, and the correct, transactions. After the validation of the master hash, the node switches it's state back to *participating*. In the *participating* state the node actively participates in the consensus.

6. Roadmap

There is constant change in the crypto space. Providing a timeline in a static paper does not allow us to keep pace with this change. What may seem the best short-term goal today might not be the most appropriate short-term goal tomorrow. For this reason, we have moved the Tixl roadmap to a web-based version where it can be adjusted as changes happen.

The roadmap can be found at https://github.com/tixl/tixl-roadmap and is also linked from the Tixl website. Using a version control system for the roadmap provides even more transparency because all updates will be visible in the changelog.

6.1 Vision

Tixl's vision is to be become the world's most advanced digital asset.

6.2 Mission

Tixl plans to achieve its vision by focusing on four main areas:

1. Proving a solid software base for the Tixl network
2. Implementing a strong marketing strategy to promote Tixl as a digital asset on public markets
3. Decentralizing the Tixl network
4. On-boarding quality, strategic partners - including exchanges, payment providers and other institutions

6.3 Marketing Strategy

As seen with Bitcoin, it is not always about having the very best technical solution. Ultimately, what counts is the network effect and the hype surrounding a digital asset. That does not mean that tech is not essential, but more that no matter how good the tech is, a project will not work with bad marketing.

When describing the marketing strategy for Tixl, we have to clarify how the success of potential marketing campaigns will be measured. Since the Tixl gGmbH does not have the goal to make profits by sales, a different way of measuring success must be established. For Tixl, KPIs for a successful marketing campaign are:

- An increase in the Tixl market price[97]
- An increase of the Tixl trading volume
- Successful token sales by the Tixl gGmbH
- Growth of the Tixl community, e.g. on Telegram and Discord
- Growth of the Tixl social media followers, e.g on Twitter and Reddit

Having defined the desired outcome of Tixl's marketing efforts, the Tixl marketing strategy is based on the following sub-strategies.

6.3.1 Limitation of Supply

The Tixl token supply is set at a maximum of 900,000 MTXLT. 43,739 MTXLT are in circulation as at October 20, 2019. That means there is currently less than 5% of the total supply in the hands of investors and over 95% in the hands of the Tixl gGmbH and its founders. This ratio is comparable to other crypto projects such as Ripple, where the parent company - Ripple - holds almost 60% of its digital asset - XRP. This situation is often criticized because when a very large portion of a decentralized asset is held by a single entity, that results in centralization because that entity has such a big influence on the market. From Tixl's point of view that criticism is entirely valid. However, what it does provide is long-term fundraising opportunities. In addition, by gradually increasing the supply and carrying out marketing at the same time, a situation can be created where demand is higher than the supply, resulting in an increase in market price. As always, there is no guarantee that by following this strategy Tixl will increase in value.

6.3.2 Influencer Marketing

Due to digital assets being a relatively new asset class, they hold a good deal of interest for the younger, "digital native" generation. This generation gets information through modern media e.g. YouTube. There are several "crypto influencers" on YouTube and videos about digital assets like Bitcoin are uploaded daily. Some of these influencers also promote new assets like Tixl.

The strategy is to work with influencers that not only promote Tixl in return for payment, but also to find influencers that believe in the Tixl project and are interested in a long-term partnership.

The frequency and amount of influencer campaigns may vary over the duration of the project. The Tixl KPIs from the first two fundraising rounds prove that influencer marketing is much more effective in a bullish market, or at least bullish market phases.

[97] The Tixl market price can be tracked on https://tixl.me/tokenomics/.

6.3.3 Investor/Advisor Marketing

Acquiring investors and on-boarding advisors it not only good for raising funds, but also for getting help with the project development.

Finding strategic investors has great flow-on benefits for the marketing of the project. These type of investors are commonly in contact with other investors like Venture Capitalists or investment arms of larger companies. Through these networks other potential investors are exposed to Tixl, and may invest as a result.

The same potential benefits are associated with advisors since they are often well connected to other potential advisors or investors.

Another advantage of acquiring investors or advisors who are prominent in the crypto space (or well known in general) is that they bring legitimacy to the project simply by way of their association with it.

6.3.4 Crypto and Business Magazines

There are many investors searching for new investment opportunities. In addition to getting information from influencers on social media, a lot of people read about digital assets in specialized or general business magazines.

Publishing articles in different magazines is certainly an option for the Tixl Project but ultimately the decision comes down to the cost-benefit of doing so. We have to consider factors such as the market situation and the potential reach of a press release or other sponsored articles. The longer-term goal is to have magazines report on Tixl without being paid to do it.

6.3.5 Exchange Listings

Having Tixl listed on an exchange is positive as it not only brings new liquidity into the market, but also increases awareness which helps attract new people to the project.

The process of getting listed on a new exchange is not easy, and the timing has to be right. There are multiple challenges associated with getting listed on a new exchange. First is the price negotiation. Different exchanges charge different listing fees for new tokens. Even though an offer might be tempting because a potential exchange has a high trading volume, it does not make sense to commit 5% of the project's funds to single listing. High volume exchanges often require a project to do market making through a professional market making company[98]. The extra costs associated mean the listing fee can easily double. In addition, exchanges are always interested in acquiring new users/traders and so often require new projects to actively carry out marketing in relation to the new listing. These marketing efforts add to the cost. If the raw

[98]Market making explanation: https://www.investopedia.com/terms/m/marketmaker.asp

listing fee for an exchange is $25,000, the overall costs - including the expenses above - may well exceed $75,000.

6.3.6 Events

It is the Tixl team's philosophy to only attend blockchain/crypto conferences if we can see a benefit to the project. Industry events are useful for meeting new people and sourcing potential new investors but they come at the cost of time. As with exchange listings, any attendance at future events will be carefully considered. We will choose to attend events if there is a high probability that new people can be brought into the Tixl project, or new investors and/or advisors can be acquired.

6.3.7 Partnerships

The longer-term goal is to establish partnerships with exchanges, payment providers and larger institutions in general. It is unlikely that these partnerships will be attained in the short-term as Tixl is still a relatively small project and a low volume/low market cap digital asset. However, the future establishment of mutually beneficial partnerships is a key goal for the project.

6.4 Open Source

The current plan is that all the components of Tixl's software required to run and operate the network will be released open source in the mid-term. The key reason that we haven't released them open source from the beginning is due to the potential for competitors to copy Tixl. We accept that it is likely that Tixl will be copied at a later stage, but the likelihood of it being financially viable for a competitor to do so is much lower if Tixl is already in widespread use. Not releasing open source now also protects Tixl's early investors.

6.5 Updates/Communication

To stay up to date with the Tixl project please join our Discord server at https://discord.gg/dzVzMdp or our Telegram group at https://t.me/tixlcurrency.

7. Risks

The risks listed below represent those considered material at the time this document was prepared. All risks presented may occur in isolation but could potentially happen at the same time, and to varying degrees of severity. The threat of these risks could have a negative affect on the Tixl project and cause doubts for prospective buyers. International incidents such as a global financial, currency and/or economic crises may also occur and exacerbate the risks outlined below.

Personal and economic circumstances unique to a buyer cannot be quantified but may amplify the effects of the risks listed.

No definitive 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 of their probability of occurrence, or the extent of their potential impact. For the sake of clarity, the following presentation is thematically structured, whereby it should 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 also have a negative impact on the Tixl Project.

The risks described below may not only have an affect on the immediate value of the Tixl Token (TXLT), but also cause Tixl (TXL) to develop negatively and lead to a partial, or complete, loss of the capital invested by 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. The risks cannot be ruled out that there may be security gaps or other errors in the applied technologies used, or faulty compilations thereof. While these risks may be offset by the implementation of security audits, for example, there is never one hundred percent certainty in computer science and cryptography. Two scenarios in particular would have a drastic effect on the price of Tixl.

Scenario 1 would be a breakup of the cryptographic system. In a worst case, an attacker could gain complete access to any number of Tixl. This would more than 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 an extended period of time for which no immediate solution can be found. Again, a long-term price collapse would result.

Advanced technical precautions are employed to safeguard against both these scenarios, thereby limiting the chances of them occurring.

7.2 Marketing Dissemination

The success of any product, including digital assets, depends on their dissemination. Theoretically, it could transpire that none of the marketing measures implemented have any effect and no further users or B2B partnerships are able to be generated. In this case, the corporate capital would eventually run out, thus rendering Tixl marketing financially impossible. This could lead to a long-term, and rather slow, drop in price.

7.3 Regulation

Governments and state institutions, whether in Germany or elsewhere in Europe, will focus more on digital assets over the coming years. This will lead to more regulation in what is currently a relatively unregulated market. The founding team is very open to cooperation with the German state, as well as other states. Tixl will definitely not look to become an *underground currency*, but instead seeks to comply with the regulations set forth in prevailing public policy (provided these do not completely block the Tixl core concept). The worst scenario 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 price.

7.4 Competition

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

Other competition comes from improvement in the usability of existing digital assets, and their distribution will increase. The key currency is likely to remain Bitcoin. As seen in the past, the next crypto-bull market will favor the competitive drive and growth of new digital assets. However, developing and launching a new digital asset gets more difficult every year.

7.5 Key Individuals Risk

The development and economic success of the Tixl project depends, to a large extent, on the experience and competence/skills 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 and economic success of the Tixl project may deteriorate, or even cease, as a result. 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 cannot be ruled out that the partners involved (as well as persons associated with them) could launch projects which compete with Tixl 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 which exposes it to all of the common risks associated with business transactions. A company always has the potential of becoming insolvent. 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 scheme. In the event of insolvency, the project's success 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. It is important to note that 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 a sale will be possible at the desired time or under 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 may make decisions which do not correspond to the objectives of the individual buyers of the TXLT and these may affect them in a negative way.

7.10 Contract Performance Risk (Counterparty Risk)

The Tixl project is based on various contractual relationships that have been established, or are yet to be established. There is a risk that the contractual partners will not meet the obligations associated with these contracts (intentionally or negligently) or will no longer be in a position to duly fulfil the contract, 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 in the market, or procured under conditions not as favorable. It must be understood 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, digital assets, and ICOs may deteriorate with individual interest groups or with society as a whole, e.g. due to a large number of unrealized projects, fraudulent or other illegal behaviour, or serious technical inadequacies (e.g. security gaps, hacks, data loss). The result of these events, either systemic or at the company level, may adversely affect the reputation of the Tixl gGmbH in terms of performance, competence, integrity and creditworthiness. A deterioration in the company's reputation would typically have a detrimental effect on the customer base and the company's business activity.

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.

TXLT
During the ICO no actual TXL, but instead Tixl tokens (named TXLT), will be available for sale on the Binance Chain. To receive TXLT, a Binance Chain wallet is required. These tokens are effectively vouchers for TXL which can be swapped for the tokens at a later stage, when the Tixl network is launched.

MTXLT
1,000,000 (one million) TXLT. MTXLT is also designed to be used as a shortcode, or symbol, on exchanges.

General Glossary

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

BEP2
BEP2 is a token standard for tokens on the Binance Chain.

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 by way of tokens. For Tixl, developer bounties as well as marketing bounties are considered.

Bounty Campaign Vesting Period
The period of 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.[99]

Decentralized Exchange (DEX)
Decentralized Exchanges allow peer-to-peer trading without a central authority.

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.[100]

ECDLP

[99] Cryptocurrency: https://en.wikipedia.org/wiki/Cryptocurrency
[100] Discord Messaging Platform: https://discordapp.com

ECDLP is the abbreviation for Elliptic Curve Discrete Logarithm Problem. The difficulty of solving the discrete logarithm problem is essential for security.[101]

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.[102]

Fiat Money
Fiat money usually refers to classic currencies such as the US-Dollar or the Euro.[103]

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.

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

Proof of Work (PoW)
Proof of Work is a consensus algorithm used e.g. by Bitcoin, to decide which transactions are valid and 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."[104]

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."[105]

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.

---

[101] Discrete Logarithm Problem: http://wiki.c2.com/?DiscreteLogarithmProblem
[102] Shaan Ray | Federated Byzantine Agreement: https://towardsdatascience.com/federated-byzantine-agreement-24ec57bf36e0
[103] Fiat: https://en.wikipedia.org/wiki/Fiat_money
[104] 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
[105] Ethereum Proof of Stake FAQ: https://github.com/ethereum/wiki/wiki/Proof-of-Stake-FAQ#what-is-proof-of-stake

Quantum Computing
Quantum computing is the use of quantum-mechanical phenomena such as superposition and entanglement to perform computation. The concept of quantum computers has existed for a long time and, in recent years, some of the tech giants have started to make practical progress on them. And while the advent of a practical, usable, functioning, well-programmed quantum computer may may not occur in the immediate to mid-term, its ramifications are already being considered by the cryptographic community. Peter Shor invented an algorithm (named Shor's algorithm), which uses the theoretical power of a quantum computer to solve the factorization problem.[106]

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.[107]

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