tokrex

Imagine a world without central crypto exchanges.

This white paper shows a highly innovative core technology that will probably have the biggest impact on how we will trade Crypto Coins in the future.

www.tokrex.org

tokrex

Executive Summary

Today, 98% of decentralized cryptocurrencies are traded on central crypto exchanges. Central exchanges favor fraud, theft and price manipulation in connection with cryptocurrencies and assets. In 2018 alone, users suffered damage amounting to almost one billion US dollars. The users of cryptocurrencies suffer from the losses and centralization. In addition, central crypto exchanges are slowing the growth of the overall market. Although institutional investors and fund managers are fond of crypto investments, they are still deterred by the "Wild West" character and the theft risk of the central crypto exchanges.

There were first technical developments to completely decentralize the trading of crypto assets and currencies and thus to eliminate the central crypto exchanges and the associated problems. However, these concepts fail due to problems such as block latency. As a result, trade executions took up to half an hour or longer, making the previous solutions unsuitable for practical use. In addition, trading cryptos for fiat money has not been satisfactorily resolved, although the demand for it is growing steadily. This development reflects the current situation of blockchain technology. Important core technologies are still missing to make the crypto market suitable for the mass market and to unleash its considerable potential.

tokrex

Tokrex is committed to fully decentralize the crypto exchange market, which has an annual volume of $2200 billion. The market must be professionalized, and the risks must be eliminated.

Three researchers succeeded in developing a cryptographic solution that enables the exchange of cryptocurrency completely decentralized and above all in real time. This allows crypto assets and currencies to flow as barrier-free and fast as data between different blockchains. The core technology, which they called Tokrex, can completely solve the problems of decentralized trading for the first time. The researchers formed the Tokrex Foundation. The innovation also solves another current and major problem of blockchains: scaling. For the first time, cryptocurrencies, such as a bitcoin, can be exchanged decentrally within a blockchain or between different blockchains in less than one second. Supported by the innovation push, the Tokrex researchers were able to develop a decentralized crypto/fiat money trading for the first time and thus present the safest alternative to the central crypto exchanges and solve the decentralized fiat/crypto trading.

The Tokrex Foundation has a knowledge and technology portfolio that provides a professional ecosystem for complete, decentralized trading of cryptocurrencies and assets. Tokrex is committed to fully decentralize the crypto exchange market, which has an annual volume of $2200 billion. The market must be professionalized, and the risks must be eliminated.

The painful path of the crypto market into centralization.

The pioneering work on crypto-currencies dates back to a group of cryptographers in the `90s known as the „Cypher-punks". Timothy C. May, Eric Hughes and John Gilmore were the visionaries of cryptocurrencies. Their idea was a complete decentralization of currencies, which should contribute to more personal freedom, privacy and independence from state influence.

The first companies with commercial interest in cryptocurrencies were crypto exchanges. Crypto exchanges today make several trillion dollars a year in revenue and have become central cryptocurrency repositories. This centralization is a major cause of crime and manipulation related to cryptocurrencies.

33% of all central crypto exchanges lost customer deposits or are subject to suspected fraud

Tyler Moore, assistant professor of cybersecurity at Tulsa Uni- versity and others, researched 80 Bitcoin exchanges. They came to the conclusion that 33% of all Bitcoin exchanges were either robbed or there was fraud by the operators of the exchanges. The problem is bigger than ever. In January 2018, cryptocurrencies worth $ 523,000,000 were stolen from the Japanese Crypto Exchange Coincheck. On June 10, 2018, the South Korean Crypto Exch-

In the vast majority of cases, customers suffered a total loss caused by the central exchanges.
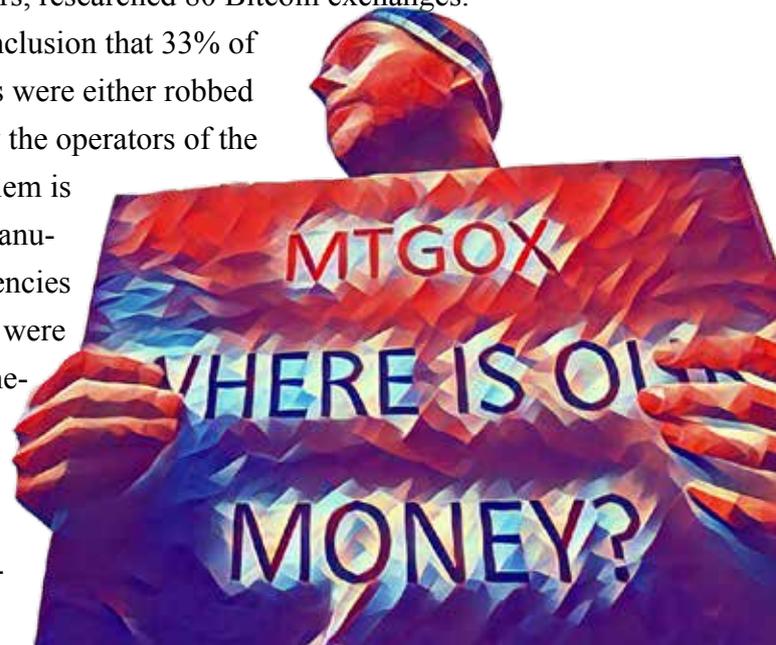
ange Coinrail lost about $ 45,000,000. Only 9 days later, the Crypto Exchange Bitthumb lost about 30,000,000 US dollars. And these are just examples from the recent past! In the vast majority of cases, customers suffered a total loss caused by the central exchanges.

Price manipulation on a large scale

A new level of crime was revealed by John M. Griffen and Amin Shams of the University of Texas-Austin with a study on the cryptocurrency Tether. The study suggested that Tether has artificially created the price increase of Bitcoins end of 2017 due to price manipulation, so by fraud. Their analysis challenged the crypto community on how many of the alleged thefts of cryptocurrencies were actually caused by unknown hackers or to what extent these „hacks" served the benefit of the exchange operators. A unique property of a blockchain is that it can store and transfer values without a trusted third party. The events of recent times show that trustworthy third parties, the central crypto exchanges, are very questionable.

Total state control

As a consequence of centralization, governments can use central crypto exchanges to fully control or shut down the crypto market, as happened in China. The independence of cryptocurrencies and the privacy of users is lost.

Block latency is the main reason for centralization

The term „digital currency" suggests that you can exchange digital currency as fast as an e-mail. However, this is not the case since a blockchain uses a time delay to cryptographically secure transactions, the so-called block latency. An opinion analysis from the Bitcoin Forum shows that block latency is the main reason why most users keep their coins on central exchanges.

Survey shows that block latency is the main reason why most users leave their coins on central exchanges.

tokrex

Blockchain's character should bring freedom

From this painful development of the crypto market, the idea of a decentralized exchange (DEX) was already born in 2014. A exchange that works without a trusted third party should revolutionize the crypto trade. The first work on this topic goes back to J.R. Willet.

Previous solutions have problems

Over time, some solutions were developed to implement a decentralized exchange, but they created new problems. Here are the main problems of the previous solutions:

■ Speed
A major problem with previous solutions is the trading speed, which is far too slow.

■ Restrictions on tradable assets
Some solutions allow only an intra-chain trade, such as Ether-Delta or WaveDEX. So only certain digital assets of a particular blockchain can be traded (like ERC20 tokens). The market share of these solutions in crypto trading is less than 2% and shows that the need for diversity can not be met by intra-chain trading.

These problems led to a low prevalence of decentralized solutions.

■ Cross-Chain-Swaps
Users have a need to trade digital assets and currencies between different blockchains, e.g. Bitcoin against Ethereum. Atomic cross-chain swaps are promising, but require technical adjustments to existing blockchain technologies, which is difficult given the high number of blockchains. In addition, they can not solve the block latency problem.

■ No fiat / crypto trade
Since many investors still do not own cryptocurrencies, there is a need for trading between Fiat and crypto money, which is not addressed by the previous solutions.

The heyday of crypto centralization

These problems led to a low prevalence of decentralized solutions. Another development are hybrid exchanges, which want to connect the two worlds together. However, they require a trusted third party and have the same problems as central crypto exchanges (price manipulation, fraud, etc). Although cryptocurrencies are inherently decentralized, we are experiencing the heyday of crypto-centralization, which threatens cryptocurrencies because decentralized trade has not been resolved.

Imagine a world without central crypto exchanges.

At the touch of a button you enter the largest independent trading floor in the world. All users trade directly among themselves, completely decentralized and distributed all over the world. In your new world, you don't trust anyone. Nobody keeps your coins. Only you have full control over your assets.

No one can scam or steal from you, because intermediaries have been replaced by well-founded cryptography. You trade your assets in the millisecond range (Tokrex). No matter if you trade coins against coins or Fiat against coins. There is also no one who keeps the pricing or a central order book. The decentralized network was modeled after the model of floor trading

and thus a completely decentralized order matching is possible (FloorNet). This way you can be sure that you are trading in a fair environment that nobody can influence.

Your new world offers real-time settlement. After a trade your coins, tokens and your Fiat money are immediately in your own wallet. Not in anyone's wallet, just on your device and safely under your control. You can withdraw Fiat money at any time through Tokrex Clearing Service Provider (CSP) or keep it in the Clearing Blockchain. Even a CSP is secure, because it does not store cryptos, but only manages bank money. Everything is done in real time. Everyone can create new markets here. Coins and tokens, even those of new blockchains or ICOs, are traded here immediately.

For your security, the decentralized system also performs Customer Due Diligence (KYC) so that you always comply with the laws (AML/CFT) of your country. Even if you want to transfer a bitcoin e.g. in a few milliseconds to your friend, you are right here. The term "central crypto exchange" is no longer known in the new world, because your personal freedom and security is the first priority here.

tokrex

Your coins are faster than you can say „wow".

Instead of transferring cryptocurrencies via on-chain transactions that are subject to long block latency, Tokrex introduces Cryptographic Deposit Guarantees that allow a quick exchange of ownership of assets. For the first time, users are able to trade or exchange cryptocurrencies directly peer-to-peer, regardless of the block time of the underlying blockchains.

On a route between New York and Paris, the execution time is 657 milliseconds.

New York – Paris in 657 milliseconds
The block latency is completely eliminated and the exchange of cryptocurrencies can take in less than a second. If one party is located in London and another in Madrid, which corresponds to a distance of about 1,300 kilometers, then an exchange takes place in about 153 milliseconds. On a route between New York and Paris, the execution time is 657 milliseconds. In comparison, it takes about 1000 milliseconds to say the word „wow" or flick your fingers. Tokrex is a real-time system according to DIN 44300 and allows a constant runtime for a unidirectional and bidirectional exchange of coins.

In Tokrex hard assets are traded
Cryptographic deposit guarantees hold real assets or coins. In fact, it is a distributed private key that gives access to real assets. It is not a replacement token as with other solutions. As long as assets or coins are tied into a cryptographic deposit guarantee, they can be exchanged in real-time across any number of parties. If a party opens a deposit guarantee, it will receive the private key for their coins or assets on average within 1.8 seconds. This is called real-time settlement. Real-time settlement does not generate any block latency.

tokrex

Intra- and Cross-Chain

With Tokrex, crypto coins can be transferred between different blockchains (cross-chain) or within a blockchain (intra-chain) in real time.

The time measurements are based on the first prototypes of Tokrex. Calculated values were calculated using a conservative model suitable for a highly scaled, decentralized network. Details can be found in the paper "Tokrex: A Metasystem for Real-time Intra- and Cross-Chain Swaps", Appendix A.

tokrex

Imagine your coins are surfing from Blockchain to Blockchain.

Tokrex uses a commonality of all blockchains, the asymmetric cryptography and can thus keep almost any cryptocurrency in a cryptographic deposit guarantee, making it tradable and securely transferable in real time. This allows coins to be easily exchanged from blockchain to blockchain without block latency. For the first time, real-time cross-chain swaps between hundreds of coins get possible. This allows an almost unlimited variety of tradable coins and assets in Tokrex. Cross-chain swaps on this scale were previously not possible, which is why Tokrex is a technological breakthrough.

No blockchain support required

The real-time transfer of blockchain assets is achieved in Tokrex without any technical adaptation of existing blockchain technology, as each blockchains uses asymmetric cryptography. This results in rapid integration of blockchains and cryptocurrencies, resulting in a huge variety of tradable cryptocurrencies. Limitations of previous DEX solutions to certain cryptocurrencies or assets, such as EtherDelta, WaveDEX or AirSwap do not exist in Tokrex.

Multiple times without any block latency

If a coin or token is bound in a cryptographic deposit guarantee, it can be traded or exchanged multiple times without block latency among any parties. There is no more block latency, as in previous solutions. Not even if a deposit guarantee is opened. This is in line with the expectations of crypto traders and users who want to trade or swap their coins quickly between different parties.

tokrex

No limits

An exchange or trade in Tokrex is done directly between the peers with very little communication complexity. There is no bottleneck, which means Tokrex can handle an almost unlimited number of transactions between peers and increase the often limited scaling of blockchains.

„Tokrex is a meta-system for blockchains that increases the scalability of a blockchain, accelerates its transaction speed to high-speed, and enables interoperability between different blockchains."
Tom M. Mayer

tokrex

Imagine, there is no order book just loud shouting.

The largest trading network in the world needs real-time trading and a powerful system to bring buyers and sellers together in a matter of seconds.

Fully decentralized order matching based on the model of floor trading.

The field of research on decentralized order matching is largely untapped. In recent decades, computer science has concentrated mainly on central systems that are unsuitable for a global decentralized network such as Tokrex.

Floor trading was a role model

For this reason, Tom M. Mayer, Christoph Mai and Jesse N. once again broke new ground and found a role model in floor trading. They modelled floor trading on a decentralized network and simulated it with real data from GDAX and Binance. Finally, they developed a decentralized synchronous broadcasting network that enables direct peer-to-peer order matching in a high-speed setting without a central order book. They called it FloorNet.

The FloorNet complements Tokrex to a completely decentralized trading floor and has outstanding performance features:

■ Unlimited parallelization - any number of buyers and sellers can be merged simultaneously, resulting in high data throughput.

■ Superb reliability

It is fail-safe and can be scaled almost indefinitely.

■ Order types

It enables any order type with partial execution:

- Limit Order
- Market Order
- Partial executions
- Order additions (like Fill-Or-Kill, etc.)

■ Decentralized matching logic

The FloorNet relocates the matching logic to the traders and allows a great flexibility in the design of order types, as well as a simple, decentralized extension of the matching logic.

■ Online and Offline Matching

FloorNet allows orders to be executed when a party is connected to the network or disconnected from the network.

■ Open market and Over-The-Counter

In principle Tokrex is a public market. In addition, a private execution is also possible.

tokrex

Imagine a world where your coins become cash in the safest way.

The trade between crypto money and fiat money is a crucial factor that has contributed to crypto centralization. For this reason, Tokrex has developed a pragmatic and secure solution that enables trading between crypto and fiat money in a decentralized trading environment without centralized exchanges.

Crypto Exchange without cryptocurrencies

Tokrex Clearing Services are companies that settle coin transactions in fiat money. However, they do not keep any coins themselves. Trading execution and delivery of assets are outsourced to the decentralized Tokrex network. They are, so to speak, crypto exchanges without cryo-currencies. They act as regulated trustees and they are the safest alternative to central exchanges.

■ Only Fiat

Tokrex Clearing Services only execute transactions in fiat money.

■ No storage of coins

Tokrex Clearing Services do not preserve cryptocurrencies because the exchange of coins is outsourced to Tokrex.

■ No central pricing

Tokrex Clearing Services outsource order matching and pricing to the decentralized order matching of FloorNet.

A Clearing Blockchain instead of blind trust

On a clearing service only fiat money can deposited and withdrawn. If a user has credit from a clearing service, they can

tokrex

use it to make fiat / crypto transactions through Tokrex. All transactions are handled via a public clearing blockchain. The Clearing Blockchain logs all deposit, withdrawal and trading activities of a clearing service.

When performing a Fiat / Crypto transaction via Tokrex, the trading parties include the Clearing Service and jointly sign the transaction on the Clearing Blockchain. Credit resulting from the Clearing Blockchain are paid out to the Tokrex users by the Clearing Service via the banking system.

Tokrex clearing services are the most secure way to trade crypto versus fiat money.

An example outlined briefly:

■ Alice deposits $ 1,100 on a Tokrex clearing service through the banking system.

■ The clearing service signs the deposit on the clearing block-chain as soon as it clears the credit.

■ If Alice buys two Ethereum for $ 1,100 from Bob through Tokrex, Bob gets credit on the clearing blockchain and Alice immediately gets the private key to the Ethereum from Bob.

■ Afterwards, Bob has a $ 1,100 balance on the Clearing Blockchain and Alice has the two Ethereum.

■ Bob can now use his private key to prove the ownership of $ 1,100 through the Clearing Blockchain. Therefore, the Tokrex Clearing Service pays the balance to Bob through the banking system.

Decentralized settlement
The exchange of assets is carried out directly between the trading parties peer-to-peer via Tokrex. The Clearing Service

has no access to the assets at anytime and is only used for the clearing of the Fiat.

Global access
The Clearing Blockchain will allow users to use different Tokrex Clearing Services in different countries as Clearing Services can clear each other.

Positive money as a model
In order to protect the Tokrex Clearing Services against payment defaults and to prevent tampering, a security deposit amounting to the maximum trading volume of a Tokrex Clearing Service is proposed, which is based on a positve money system. The security deposit is secured by group trustees (CTAs). The maximum trading volume of a clearing service based on the security deposit can be publicly traced and controlled via the clearing blockchain.

Tokrex Clearing Services are an optional building block of the Tokrex system to enable secure and decentralized trading of Fiat money and Crypto money.

tokrex

Be infinitely creative: trade what you like!

Everyone can create markets or financial instruments. Tokrex is designed solely by the creativity of its users and open source community.

Everyone can create markets or financial instruments in Tokrex. Tokrex is designed solely by the creativity of its users and open source community.

■ Coins become accessible to everyone faster.
No one has to wait until coins are listed on a crypto exchange, because every user can offer new coins or tokens.

■ Fast liquidity for new coins and tokens
Offering new assets on the market is cost-neutral and effortless.

■ Illiquid assets
No one can fool coins. As long as there is an offer for coins you can trade.

■ New financial instruments
Tokrex allows the grouping of cryptographic deposit guarantees and thus the creation of index and fund instruments by each user. One example is cryptographic real estate funds, which consist of blockchain assets that map land titles.

Scientific papers and video & live presentation.

The scientific papers on Tokrex and FloorNet as well as video presentations can be found here:

Tokrex: Metasystem for real-time intra- and cross-chain swaps (Mayer et al.)

A detailed description of the Tokrex crypto-system as well as the cryptography according to Mayer et al .:

Link: PDF Document

URL: https://tokrex.org/whitepaper-tokrex

Audience: Experts

FloorNet: Decentralized Order Matching (Mayer et al.)

A detailed description of the FloorNet according to Mayer et al .:

Link: PDF Document

URL: https://tokrex.org/whitepaper-floornet

Audience: Experts

Video presentation: Tokrex and FloorNet, System Design & Cryptography

An introduction to Tokrex and the FloorNet by Tom M. Mayer.

Link: Video

URL: https://tokrex.org/video-crypto

Audience: Experts

Live presentation: Tokrex in live trading

An introduction to the history of Tokrex and presentation of the Tokrex prototypes by Tom M. Mayer.

Link: Video

URL: https://tokrex.org/video-presentation

Audience: Everyone (not technical)