DRSK – Draft Whitepaper

Foreword

The DRSK vision is to enable a global decentralized marketplace that empowers participants to transfer risk peer-to-peer.

A vast range of risks cannot be protected against, thus transferred, such as non-damage business interruption, given limited access or lacking capacity.

This whitepaper describes our approach towards filling this opportunity by creating an entirely democratic ecosystem, which is secure, scalable, cost-efficient and without information asymmetry.

Although technology agnostic, the ecosystem is implemented and made available to the public on distributed ledger technology (DLT).

See cerchia.io

1 Problem statement

Risk transfer is the established practice of protection sellers providing compensation to protection buyers for losses from specified events over a certain timeframe, at agreed premia. A wide range of risk transfer products has been introduced and are transacted in volume, from simple insurance to sophisticated treaty reinsurance, catastrophe bonds, insurance-linked securities and warranties.

Whilst risk transfer products have been steadily growing in transacted volume over the years, there exist massive gaps to the tune of USD 1.4 trillion in protection for uninsurable risks such as non-damage business interruption or supply chain disruption.

Risk transfer products are costly to structure and opaque to analyse. The risk transfer process is naturally controlled "centrally" by large reinsurance companies. Hence, there could never emerge a truly "decentralized" marketplace for risk transfer, accessible to participants with varying objectives.

2 The Opportunity

We believe the future of risk transfer is decentralized, embedded in a vibrant marketplace where different participants can transfer risks directly peer-to-peer, infinitely scalable, entirely secure and automated.

A supranational and self-regulating association (DRSK) is advancing the cause for decentralized peer-to-peer risk transfer and a vital success factor to global scale. It is promoting best practices and standards for decentralized peer-to-peer risk transfer to its members. DRSK is going further by providing Direct Risk Transfer (DRT) to participants, a self-governed implementation of best practices and standards to process and settle decentralized peer-to-peer risk transfer.

For empowering and equip participants around the world with simple access to DRT, DRSK provides a free template to establish a DRT Decentralized Marketplaces (DDM).

3 Product & Organisation

3.1 Direct Risk Transfer (DRT)

DRT is a standardized contract to transfer risk peer-to-peer. As a bilaterally agreed financial derivative, the buyer and the seller ensure their own eligibility and compliance to transact such contract under respective local laws and where applicable, cross borders.

Conceptually, DRT requires a protection buyer to deposit a premium in secure escrow, and a protection seller to accept such an offer ("bid") by depositing the protection amount reduced by said premium in the same escrow. Vice versa, a protection seller can offer to sell protection by depositing a protection amount reduced by the requested premium in escrow ("ask"), and a protection buyer can accept this offer by depositing the required premium in escrow. All cash flows are settled in a limited range of stable-coins (no crypto or DRSK Tokens).

From a legal perspective, buyer and seller authorising a transaction corresponds to entering a bilateral ISDA master agreement[1] and signing a term sheet reflecting the risk being transferred.

After establishing a contract, the index specified in the contract terms is observed during the observation period. As and when this index exceeds an agreed value a payment of the full protection amount in escrow is triggered to the protection buyer. If the observation period passes without the index exceeding the agreed value, the full protection amount is paid to the protection seller. With the full protection amount securely held in (decentralized) escrow, there remains no counterparty credit risk to the transaction, and hence no margining, clearing with a central counterparty is required.

The technical implementation of DRT is automated using smart contracts on Distributed Ledger Technology (DLT), the DRT Smart Contracts. Here, simple access to a wallet allows

[1] ISDA Master Agreement - Wikipedia

protection buyers and sellers to transact peer-to-peer and settle transactions in stable-coins. Automation with smart contracts enhances the DRT contract security, tractability and efficiency for buyers and sellers. The DRT Smart Contract, like any other smart contract, is identifiable with a decentralized address on DLT, which is used as programmable escrow account. The generic DRT Smart Contracts are parametrized with a fixed set of standards ("Standards"), allowing transfer of risk in a standardized manner, eliminating paper, physical contracts and confirmations altogether. The Standards are stylized as follows:

		Country	Region	Trigger	Strikes
Geophysical	Earthquake	Japan	Prefectures	**JMA Seismic Intensity Scale**	7, 6+, 6-, 5+, 5-
		United State	7.5' 1:24'000 quadrangle	United States Geological Survey	-
	Mass Movement	...	...	...	...
	Volcanic Activity	...	...	...	...

Biological	Hydrological	Meteorological	Climatological	Anthropogenic	Extraterrestrial
Epidemic	Extreme levels	Wind	Drought	Air pollution	Impact
Animal infestation	Landslide	Extreme temperature	Glacial lake outburst	Water pollution	Space weather
	Wave action	Hail	Wildfire	Inhabitable area	
		Snow			

Each risk of the Standards is categorized (geophysical, biological, hydrological, etc) and linked to a suitable data source, used as the parametric trigger index for the DRT Smart Contracts. International and open data licences are typically a pre-requisite for a suitable data source. The Standards themselves are trademarked, with the intellectual property owned and managed by the DRSK Association.

Akin to a subscription, buyers and sellers are charged a processing fee for live DRT Smart Contracts. The processing fee is automatically deducted from the protection amount held in escrow, accruing to the DRSK Treasury.

Fall-back procedures are agreed upon upfront in the Standards, and directly programmed into the DRT Smart Contracts. For example, a data source might stop publishing the

parametric trigger index, and another source must be considered. Complete unwind could become necessary under so-called “acts of god” scenarios. Again, DRT automatically follows agreed Standards which are programmed into the DRT Smart Contracts, without any interference by external parties.

3.2 DRT Decentralized Marketplace (DDM)

A decentralized marketplace for DRT enables buyers to find sellers and vice versa, and directly enter DRT Smart Contracts without intermediaries. DDM is not a trading venue nor an exchange, as no matching or intermediation is performed. As such there exist no contractual relationship with DRSK Association or Cerchia AG. A DDM represents functionality to display DRT Smart Contract activity on DLT and is established on request with a user locally. From a legal perspective as terms of use, the risk of accessing and transacting DRT Smart Contracts using a DDM remains entirely with the user, and there remains no liability claim towards DRSK Association or Cerchia AG.

Potential liability claims with regards to DRT processing failure and their handling are described in the paragraph on DRSK Reserve.

Like a bulletin board the DDM allows to display DRT Smart Contract activity such as bids, asks, live and terminated contracts on the specific public DLT. Individual buyers and sellers of protection can publish their offers to buy (“bid”) or sell (“ask”) at a committed premium amount directly to DLT (not DDM). DDM helps to display such new DRT Smart Contract activity on DLT and interested users can then enter DRT by accepting a bid or an ask directly on DLT.

If not accepted by another party, bids and asks can be cancelled by the initiating party at any time (on DLT).

3.3 DRSK Association

The DRSK Association is a not-for-profit association established under laws of Switzerland. Operating supranationally, it pursues the mission to foster safe and efficient decentralized peer-to-peer risk transfer markets and facilitate effective risk management to all users of decentralized peer-to-peer risk transfer. DRSK aims to:

1. Be the preeminent standard for global decentralized peer-to-peer risk transfer
2. Advocate effective risk and capital management amongst decentralized peer-to-peer risk transfer participants
3. Enhance counterparty and market risk practices, and ensure a prudent and consistent regulatory framework for decentralized peer-to-peer risk transfer
4. Provide unified global standards, documentation, and implementation for decentralized peer-to-peer risk transfer, to develop and promote legal certainty and maximum risk reduction
5. Advance practices related to transacting, processing, reporting of decentralized peer-to-peer risk transfer.
6. Digitize activities, where possible and as appropriate, to reduce or eliminate operational risks.

The DRSK Association is governed by its members, completely decentralized and automated, using DLT. To power global decentralized peer-to-peer risk transfer operations, DRSK provides participants with DRT Smart Contracts, supported by an entire token economy ("DRSK Tokenomics").

3.4 DRSK Token and DRSK Tokenomics

The DRSK Token represents membership in the DRSK Association. It further carries utility as being the vital means for voting within a dedicated DRSK token economy ("DRSK

Tokenomics"). The token, however, doesn't represent any ownership on value in the DRSK Tokenomics and doesn't entitle the token holder to any claim on value against the DRSK Association or other entities.

At the outset, a fixed supply of 100 million DRSK Tokens are being minted and issued to the DRSK Association's treasury for further distribution (as per below chart). Of this total amount, 15 million DRSK were sold as part of a private sale in August 2021 (Simple Agreement for Future Tokens or "SAFT"), with funds raised for an initial implementation of DRT, DDM and DRSK. Another 20 million DRSK Tokens are allocated to incentivize technology provider Cerchia AG and will vest over 24 months. The remaining 65 million DRSK Tokens are reserved for issuance to DRSK Association members upon launch, treasury and tokenomics management.

Ticker	DRSK
Type	Utility token
Country of issuance	Switzerland
Supply	100 million (fixed)

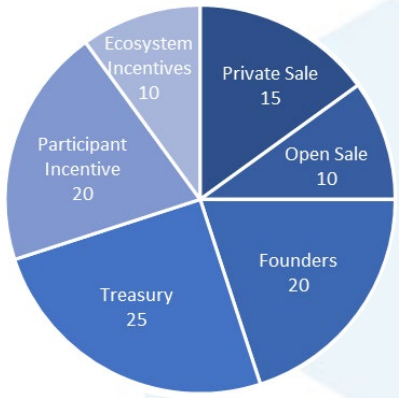

Figure 1: Allocation DRSK Token, in millions

Features of DRSK token:

- Voting in the DRSK Association
- Discretionary contribution to compensate claim validators and admitted claims against the DRSK Reserve, where funds are not recoverable
- Incentive for technology and data providers to process DRT
- Incentive for security programmes (bounties, white hacking)
- Incentive to DRSK Association members and community

3.5 DRSK Treasury

The DRSK Association balances its tokenomics with a fully autonomous and automated treasury smart contract, the "DRSK Treasury". Equipped with an initial allocation of 25 million DRSK tokens, it directs the various flows under the not-for-profit paradigm of the DRSK Association:

- Processing fees from DRT Smart Contracts denominated in a variety of possible standard tokens (in stable-coins, the income)
- Discretionary incentives (DRSK Tokens) to technology and data providers for processing DRT Smart Contracts (expense)
- Discretionary incentives (DRSK Tokens) to security providers (bounties)
- Discretionary incentives (DRSK Tokens) to DRSK Token holders for entrusting their DRSK Tokens with the DRSK Reserve (expense)

As all management of flows is pre-programmed in the DRSK Treasury smart contract, no centralized or decentralized entity, even the DRSK Association and its members, can execute control over tokens in the DRSK Tokenomics. Incentives directed by the DRSK Treasury are always denominated in DRSK Tokens. To balance the DRSK Treasury over

time, DRSK Tokens must be acquired by the DRSK Treasury in exchange for tokens (stable-coins) accumulated from DRT processing fees.

3.6 DRSK Reserve

DRT Smart Contract processing relies on the integrity and security of data and technology. If a DRT Smart Contract is wrongly triggered or settled, either party of any transaction through the affected DRT Smart Contracts might suffer a loss. The DRSK Association, through its voting mechanism using DRSK Tokens, acts as an appeal body to resolve disputed DRT Smart Contract processing failure. DRSK Token holders collectively establish a reserve pool, called the DRSK Reserve, and entrust DRSK Tokens in the DRSK Reserve's smart contract. The pool of DRSK Tokens in the DRSK Reserve can be (partially) slashed to pay out compensation claims for DRT processing failure upon acceptance by the DRSK Association through voting and validation. The DRSK Treasury can provide discretionary incentives to DRSK Token holders entrusting their DRSK Tokens with the DRSK Reserve.

3.7 DRSK Security

DRT must set the highest standards in terms of transaction security and efficiency for its participants. Hence, the DRSK Association, via DRSK Treasury, incentivizes security programs on a discretionary basis. Besides regular smart contract audits through specialists and community, dedicated bounty programs allow proactive identification of vulnerabilities and respective mitigation.

3.8 DRSK Voting

One DRSK Token reflects one member vote in the DRSK Association. Voting in the DRSK Association is required on a regular basis for:

- Ordinary elections and votes pertaining to the organisation and administration of the DRSK Association
- Proposals to determine or amend Standards for DRT
- Proposals to adapt mission, strategy, and its underlying technological implementation
- Collaboration and extensions of contracts with partners, such as Cerchia AG as the initial exclusive technology provider (locked in for 3 years)
- Resolution of appeals by DRT users to claim against the DRSK Reserve

There is no voting on any financial or token flows in the DRSK Tokenomics, DRSK Treasury, or execution/processing of DRT Smart Contracts.

3.9 Member Registration for DRSK Association

Only DRSK Token holders registering and verifying their identity[2] with the DRSK Association are eligible for voting (decentralized member registry). After successful verification of a valid and recognised digital identity, and the proof of DRSK Token holdings, an NFT is minted. This NFT contains references to the identity and the token account. Only such NFT together with corresponding DRSK Token balance above a certain threshold allows to participate in the voting process.

To avoid concentration of voting power, duplication of votes or counting of marginal sleeping accounts, only circulating DRSK Tokens are eligible in a vote (DRSK Treasury is

[2] https://www.enisa.europa.eu/publications/digital-identity-leveraging-the-ssi-concept-to-build-trust

excluded), and both a cap and a floor on amounts of DRSK Tokens applies on voting from individual DRSK Token holders.

3.10 Risk Management & Regulatory Environment

Various national and supranational regulations apply to OTC transactions of derivatives. These regulations aim to provide a safe, fair and transparent marketplace for such transactions. ISDA master agreements are the globally accepted legal framework and documentation to transact OTC derivatives. DRT is thus subject to regulations in individual countries, where DRT participants, financial and non-financial entities, must comply with their applicable laws and regulations individually.

Beyond local laws and regulations of its members and participants locally, the DRSK association overlays additional self-regulating mechanisms to assure stakeholders of achieving its mission for safe and efficient decentralized global peer-to-peer risk transfer.

As a self-regulating body the DRSK Association establishes and enables through member voting:

- Appeal body for transaction processing failures
- Reserve to compensate participants for transaction processing failures
- Sanctioning of data and technology providers
- Blacklisting of DRSK Association members
- Incentive programs for security providers
- Special audits and taskforces, as and when applicable

The actual implementation of DRT eliminates inherent risks of over-the-counter (OTC) transactions, namely:

- Counterparty credit risk and clearing risk is eliminated with smart contracts acting as decentralized escrow accounts
- Settlement risk is eliminated with complete pre-programmed automation of the contract terms, including fallback procedures
- Operational risk is eliminated with complete transaction autonomy and decentralization
- Legal risk is eliminated by using the ISDA master agreement framework
- Compliance risk is eliminated as individual members and participants comply with their applicable laws and regulations
- Sanctions and travel rule are enforced by using locally licensed e-money issuers at the fiat conversion point of respective stable-coins
- Money laundering, terrorism financing, embezzlement and theft are mitigated with public blockchain tractability and auditability

4 Technical Part

4.1 DRT & Blockchain

The underlying blockchain of the DRSK Association is Zilliqa.

Building Blocks	Name / Reference
Blockchain	Zilliqa (*zilliqa.com;*Zilliqa Team, 2017)
Blockchain Coin	ZIL (Zilliqa Team, 2017)
Smart Contract Language	Scilla (*Scilla Language Implementation*)
Token	DRSK, ZRC-2 (Zilliqa, 2021)

Zilliqa is a next generation blockchain, which was designed and built with security in mind. Its main differentiating features to other blockchains are fast transactions, low transaction costs and a secure smart contract language.

The DRSK token is based on to the ZRC-2 standard (Zilliqa Reference Contracts).

4.2 Governance Processes

4.2.1 Community Proposals

DRSK Token holders can suggest a DRSK Community Proposal (DCP, see section 4.4). All proposals must be consistent with the goals and values of the community. The purpose of the DCP is to provide a structured process for extending the functionality of DRT and proposing the integration of new indexes.

The governance process is required to approve or reject proposed changes in a structured and comprehensible way by all DRSK Association participants.

4.2.2 Compensation Claim Process

DRT relies on oracle integrity. If an oracle malfunctions or delivers incorrect data, a DRT transaction could be wrongly triggered (or not triggered at all). In such a case, either party of the affected transactions can claim compensation from the DRSK Reserve (staking pool).

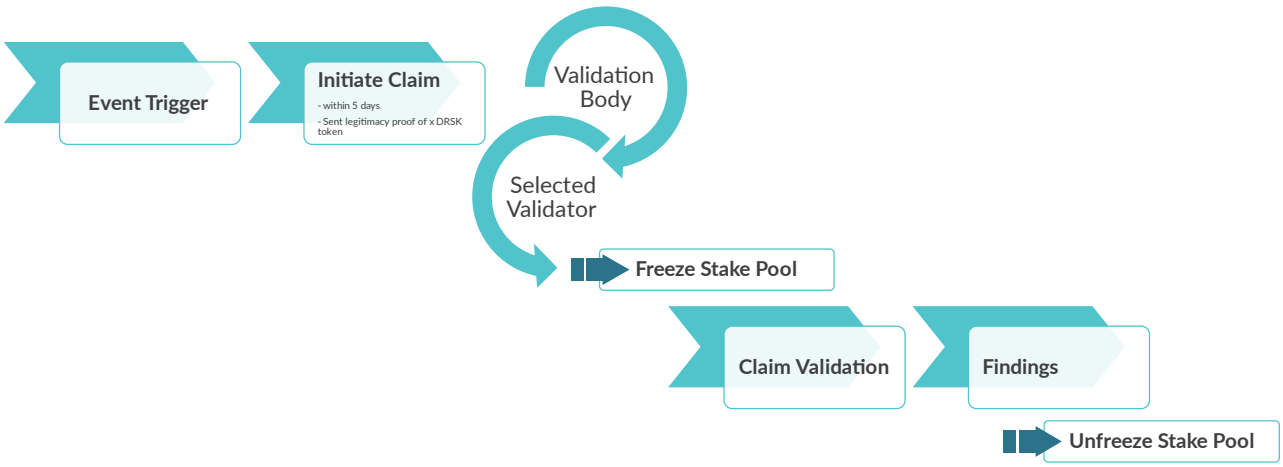

Figure 2: Compensation Claim Process

- A claim is initiated by a DRT party by sending at least [10000] DRSK Tokens to a dedicated claim address (or returning the amount wrongly received) that belongs to the staking pool and quoting the transaction ID.
- The claim is immediately rejected if such amount is below [10000] DRSK Tokens or more than [5] calendar days passed since the transactions triggered (or weren't triggered).
- Qualifying claims trigger a freeze of the staking pool during which no DRSK Tokens can be withdrawn. The claims will be reviewed by the validation body within [5] calendar days and rejected if deemed invalid.
- If the validation body deems the claim to be valid and accepted, the validation body:
    - identifies and disconnects the malfunctioning oracle node(s)
    - identifies all affected deals and addresses of participants

- sends allowance requests to addresses wrongly being paid out according to their pay-out amounts
- monitors collected amounts from addresses where allowance has been granted
- blacklists all address not granting allowance within [5] calendar days
- slashes DRSK Reserve staking pool equivalent to claimed amounts offset by returned funds, and sends DRSK Tokens to affected addresses for compensation (no conversion to settlement currencies)

- If a claim is rejected or accepted, with payments settled according to the sequence above, such claim is deemed resolved and the staking pool automatically unfrozen.
- The DRSK Treasury compensates the validation body with [x] DRSK Tokens.

4.2.3 Treasury

One or more contract(s) holding all DRSK token. The treasury is responsible for directing all in- and outflows, including staking rewards and the pay outs of accepted compensation claims.

4.3 Organization & Structure

DRSK community is a participant in the DRSK eco system. DRSK Association promotes collaboration within the DLT community and offers incentives and grants. The Validation body onboards candidates and appoints them as validator. For the claim validation, a validator is chosen randomly by the validation body. The random selection of a validator out of a candidate pool supports the unbiased processing towards the claiming party.

Cerchia AG is the solution provider of the eco system, developing, operating, integrating and maintaining the data providers operationally. Additionally, the company is commissioned with marketing, and legal services. As part of these functions, Cerchia AG

issued the DRSK Token on behalf of the DRSK Association, which is the beneficiary and main body of DRSK in charge.

In DRSK v1.0, Validation Body and Validator are represented by Cerchia AG. This will change in a later version, where the Validation Body consists of several Validators. Validators are members of the DRSK eco system.

4.4 DRSK Community Proposal (DCP) and DCP Process

The DRSK Community Proposal allows to the community to participate on the evolvement of the direct risk transfer landscape and its eco system.

DRSK Association Governance Portal (GOVP) will be reachable at gov[domain]. The portal is the main interaction interface between the DRSK community and the DRSK Association. A proposal can be submitted over GOVP and offers a forum for discussions on new submissions, as well as listings of past and ongoing proposals. Ongoing proposals are open for vote.

4.4.1 DCP

The proposal has a predefined structured with mandatory fields defined as follow:

TITLE

SUMMARY	Simple description of the outcome the proposed change intends to achieve. This should be non-technical and accessible to a casual community member.
ABSTRACT	A short (~200 word) description of the proposed change. The abstract should clearly describe the proposed change. This will be done if the DCP is implemented
MOTIVATION	This is the problem statement. This is the why of the DCP. It should clearly explain why the current state of the protocol is inadequate.

SPECIFICATION	This is a high-level overview of how the DCP will solve the problem. The overview should clearly describe how the new feature will be implemented.
DRSK ADDRESS DCP SENDER	Address to verify legitimacy of the DCP sender. Proof of legitimacy will be released after DCP validation.

Table 1: DCP Structure

4.4.2 Formal Acceptance Criteria

To restrict proposal submissions only to DRSK Token holders with legitimate interests, the submitter will be required to send [x] DRSK Tokens to the DRSK Association's DCP validation address. After the validation process, the amount is returned to the sender. The proposal has to address one or a combination acceptance criterion and not involving any of the exclusion criteria.

A DCP can reward on-/off-chain DRSK token as part of the proposal.

Table 2: Acceptance criteria (AC)

AC 0	Only whitelisted (Zilliqa) addresses are allowed to submit proposals, staked token holders can only vote on proposals
AC 1	DRT
AC 2	DRT Oracles
AC 3	DRSK Association / Governance
AC 4	DRSK eco system
AC 5	DRT Token specification/mechanics

Table 3: Exclusion criteria (EC)

EC 0	DCP is not confirming to law
EC 1	Staked token holders
EC 2	DCP not relevant to any of AC 1 / 2 / 3 / 4 / 5
EC 3	DCP involves direct DRSK pay-outs without benefits to one or a combination of AC 1 / 2 / 3 / 4 / 5

4.4.3 DCP Process

After DCP submission and the transfer of the DRSK legitimacy threshold, the DCP is validated within 3 days. A valid DCP will be published for vote.

References

Scilla Language Implementation. Available at: https://github.com/Zilliqa/scilla.
Zilliqa (2021) *ZRC-2 Token*. Available at: https://github.com/Zilliqa/ZRC/blob/master/zrcs/zrc-2.md.
Zilliqa Team (2017) *The Zilliqa Technical Whitepaper*. Available at: https://docs.zilliqa.com/whitepaper.pdf.
zilliqa.com. Available at: https://www.zilliqa.com/.
ZILO. Available at: https://docs.zilswap.io/how-to/zilo.
ZILSwap. Available at: https://zilswap.io/.