



**University  
of Basel**

Center for  
Innovative Finance

# **Smart rental deposit accounts on Ethereum**

**Matthias Nadler**

Supervised by Prof. Dr. Fabian Schär

Credit Suisse Asset Management Professor for DLT/FinTech

# Overview

## Structure of the presentation

The Problem

The Smart Contract

The Off-Chain Contract

The Interface

The Future

# Overview

## The Problem

- The zero-interest problem

- Smart contracts and stablecoins

- How to invest the deposit

## The Smart Contract

- A graphical overview

- Multisig

- Documents

- Modularity

- Security and testing

## The Off-Chain Contract

- Legal document

## The Interface

- [smartdepos.it](https://smartdepos.it)

## The Future

- What needs to be done

- Use case for the contract

# The Problem

Banks don't pay interest on rental deposits

In Switzerland, a rental deposit needs to be placed in a (savings-) account at a bank, or in a deposit on the tenants name.<sup>1</sup>

---

<sup>1</sup>OR Art. 257e para. 1

# The Problem

Banks don't pay interest on rental deposits

In Switzerland, a rental deposit needs to be placed in a (savings-) account at a bank, or in a deposit on the tenants name.<sup>1</sup>

But banks don't offer interest rates on rental deposits:<sup>2</sup>

- ▶ UBS and Credit Suisse pay 0% interest
- ▶ Raiffeisen pays 0.05% interest

---

<sup>1</sup>OR Art. 257e para. 1

<sup>2</sup>As of March 8th 2020, according to the official published rates.

# The Problem

Banks don't pay interest on rental deposits

In Switzerland, a rental deposit needs to be placed in a (savings-) account at a bank, or in a deposit on the tenants name.<sup>1</sup>

But banks don't offer interest rates on rental deposits:<sup>2</sup>

- ▶ UBS and Credit Suisse pay 0% interest
- ▶ Raiffeisen pays 0.05% interest

Is there a way we can earn interest on the deposited security without putting the landlord in a less favourable position?

---

<sup>1</sup>OR Art. 257e para. 1

<sup>2</sup>As of March 8th 2020, according to the official published rates.

# Overview

## The Problem

- The zero-interest problem

- Smart contracts and stablecoins**

- How to invest the deposit

## The Smart Contract

- A graphical overview

- Multisig

- Documents

- Modularity

- Security and testing

## The Off-Chain Contract

- Legal document

## The Interface

- smartdepos.it

## The Future

- What needs to be done

- Use case for the contract

# Smart Contracts

Deterministic code execution on the blockchain

Attempt to solve the zero-interest problem by moving the rental deposit to a smart contract on the Ethereum blockchain.



# Smart Contracts

Deterministic code execution on the blockchain

Attempt to solve the zero-interest problem by moving the rental deposit to a smart contract on the Ethereum blockchain.

The smart contract will safe-keep and invest the deposit to generate interest for the tenant while remaining in full control over the funds.

# Smart Contracts

Deterministic code execution on the blockchain

Attempt to solve the zero-interest problem by moving the rental deposit to a smart contract on the Ethereum blockchain.

The smart contract will safe-keep and invest the deposit to generate interest for the tenant while remaining in full control over the funds.

However, not everything can be solved with the smart contract. Off-chain contracts and a trustee are still necessary.

# Stablecoins

DAI instead of ETH

DAI is a decentralized crypto stablecoin with its value soft-pegged to the US dollar. Over time, 1 DAI will be equal to 1 US dollar.<sup>3</sup>

---

<sup>3</sup>In the short term, the DAI can be slightly above or below the USD

# Stablecoins

## DAI instead of ETH

DAI is a decentralized crypto stablecoin with its value soft-pegged to the US dollar. Over time, 1 DAI will be equal to 1 US dollar.<sup>3</sup>

Using DAI instead of ETH will eliminate the ETH volatility risk and allows to hold the deposit in a stable currency the same way a bank would.

---

<sup>3</sup>In the short term, the DAI can be slightly above or below the USD

# Stablecoins

## DAI instead of ETH

DAI is a decentralized crypto stablecoin with its value soft-pegged to the US dollar. Over time, 1 DAI will be equal to 1 US dollar.<sup>3</sup>

Using DAI instead of ETH will eliminate the ETH volatility risk and allows to hold the deposit in a stable currency the same way a bank would.

Most of the DeFi ecosystem is powered by stablecoins and DAI is the market leader. As of September 2019, DAI accounts for almost 90% of all loans in the DeFi ecosystem [Sch20].

---

<sup>3</sup>In the short term, the DAI can be slightly above or below the USD

# Overview

## The Problem

- The zero-interest problem

- Smart contracts and stablecoins

- How to invest the deposit

## The Smart Contract

- A graphical overview

- Multisig

- Documents

- Modularity

- Security and testing

## The Off-Chain Contract

- Legal document

## The Interface

- [smartdepos.it](https://smartdepos.it)

## The Future

- What needs to be done

- Use case for the contract

# How to invest the deposit

Minimize the risk!

- ▶ As with any investment, balance risk and return.
- ▶ Deposit is a security → strong bias for low risk.

# How to invest the deposit

Minimize the risk!

- ▶ As with any investment, balance risk and return.
- ▶ Deposit is a security → strong bias for low risk.
- ▶ DAI offers a riskless investment: The DAI saving rate (DSR).
- ▶ Alternatively, invest on a DeFi platform like rDAI.



# How to invest the deposit

Minimize the risk!

- ▶ As with any investment, balance risk and return.
- ▶ Deposit is a security → strong bias for low risk.
- ▶ DAI offers a riskless investment: The DAI saving rate (DSR).
- ▶ Alternatively, invest on a DeFi platform like rDAI.
- ▶ The difference in return is small<sup>4</sup> → choose the riskless option.

---

<sup>4</sup>March 6th: DSR 8%, rDai 8.07%. April 19th: DSR 0%, rDai 2.53%.

# How to invest the deposit?

## Riskless DSR investment

What is DSR and why is it riskless?

# How to invest the deposit?

## Riskless DSR investment

What is DSR and why is it riskless?

- ▶ DSR is a part of the MakerDAO system.
- ▶ It helps to stabilize the peg by changing the supply.

# How to invest the deposit?

## Riskless DSR investment

What is DSR and why is it riskless?

- ▶ DSR is a part of the MakerDAO system.
- ▶ It helps to stabilize the peg by changing the supply.

How does it work?

- ▶ To gain interest, your DAI is locked in a smart contract.

# How to invest the deposit?

## Riskless DSR investment

What is DSR and why is it riskless?

- ▶ DSR is a part of the MakerDAO system.
- ▶ It helps to stabilize the peg by changing the supply.

How does it work?

- ▶ To gain interest, your DAI is locked in a smart contract.
- ▶ Higher DSR → more people lock their DAI  
→ less DAI on the market → higher DAI price.

# How to invest the deposit?

## Riskless DSR investment

What is DSR and why is it riskless?

- ▶ DSR is a part of the MakerDAO system.
- ▶ It helps to stabilize the peg by changing the supply.

How does it work?

- ▶ To gain interest, your DAI is locked in a smart contract.
- ▶ Higher DSR → more people lock their DAI  
→ less DAI on the market → higher DAI price.
- ▶ Guaranteed liquidity, no dependencies and no time locks.

# Overview

## The Problem

- The zero-interest problem
- Smart contracts and stablecoins
- How to invest the deposit

## The Smart Contract

### **A graphical overview**

- Multisig
- Documents
- Modularity
- Security and testing

## The Off-Chain Contract

- Legal document

## The Interface

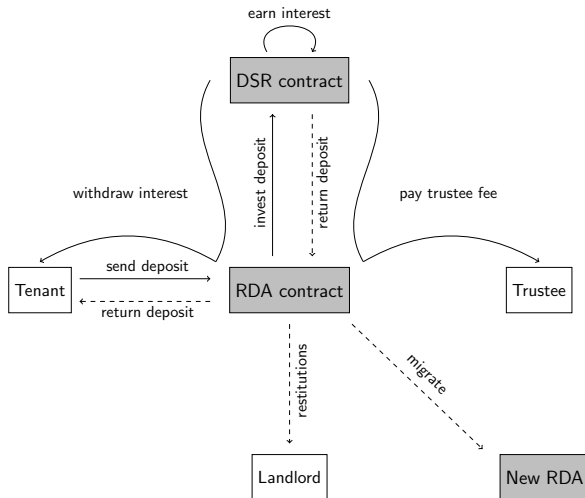
- `smartdepos.it`

## The Future

- What needs to be done
- Use case for the contract

# A graphical overview

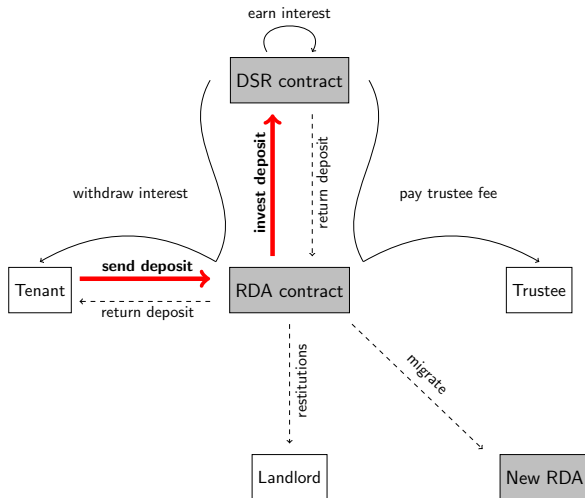
The smart contract is in control





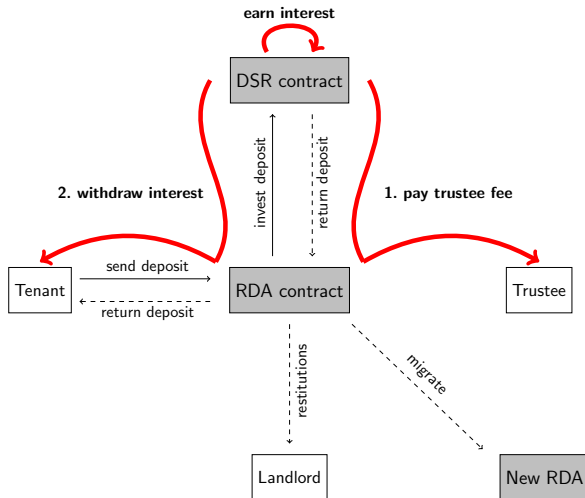
# A graphical overview

The deposit is invested by the tenant



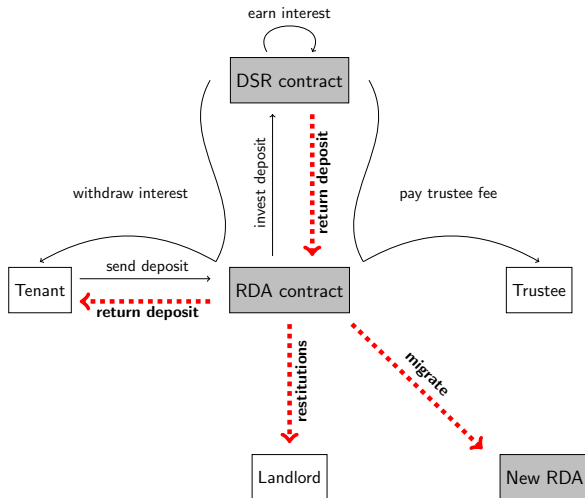
# A graphical overview

Interest is managed by the RDA contract



# A graphical overview

Dashed actions require multiple signatures



# Overview

## The Problem

- The zero-interest problem
- Smart contracts and stablecoins
- How to invest the deposit

## The Smart Contract

- A graphical overview

### **Multisig**

- Documents
- Modularity
- Security and testing

## The Off-Chain Contract

- Legal document

## The Interface

- `smartdepos.it`

## The Future

- What needs to be done
- Use case for the contract

Multisig: To execute a transaction, more than one account has to consent before it can be executed.

For this contract, a multisig transaction has to be confirmed by two out of the three participants.

# Multisig

## Introduction

Multisig: To execute a transaction, more than one account has to consent before it can be executed.

For this contract, a multisig transaction has to be confirmed by two out of the three participants.

For example: To return the deposit to the tenant, both the tenant and the landlord have to sign the transaction.

# Multisig

## Trustless interaction

We use on-chain multisig, heavily based on the proven and audited code base of the GNOSIS multisig wallet [GNO19].

The trustee in combination with multisig ensures that off-chain agreements can be enforced on the smart contract.

# Multisig

## Trustless interaction

We use on-chain multisig, heavily based on the proven and audited code base of the GNOSIS multisig wallet [GNO19].

The trustee in combination with multisig ensures that off-chain agreements can be enforced on the smart contract.

For example: A court order to release the deposit to the landlord or another requirement specified by contract law<sup>5</sup>.

---

<sup>5</sup>OR Art. 257e ff.



# Overview

## The Problem

- The zero-interest problem
- Smart contracts and stablecoins
- How to invest the deposit

## The Smart Contract

- A graphical overview
- Multisig

### **Documents**

- Modularity
- Security and testing

## The Off-Chain Contract

- Legal document

## The Interface

- `smartdepos.it`

## The Future

- What needs to be done
- Use case for the contract

# Documents

## Using multisig to sign documents

We have already implemented a robust multisig for transactions.  
We can use the same code with very little addition to digitally sign documents!

# Documents

## Using multisig to sign documents

We have already implemented a robust multisig for transactions.  
We can use the same code with very little addition to digitally sign documents!

It is possible to attach the hash of a document to an RDA contract where it can be signed by any of the three participants.

# Documents

## Using multisig to sign documents

We have already implemented a robust multisig for transactions. We can use the same code with very little addition to digitally sign documents!

It is possible to attach the hash of a document to an RDA contract where it can be signed by any of the three participants.

For example: Attach the hash of the rental contract and have it signed by the tenant and the landlord.

# Overview

## The Problem

- The zero-interest problem
- Smart contracts and stablecoins
- How to invest the deposit

## The Smart Contract

- A graphical overview
- Multisig
- Documents
- Modularity**
- Security and testing

## The Off-Chain Contract

- Legal document

## The Interface

- smartdepos.it

## The Future

- What needs to be done
- Use case for the contract

# Modularity

Factory-child pattern and interest module

New RDA contracts can be created through a factory contract which serves as a registry. Users can find all contracts involved with a specific address.

# Modularity

## Factory-child pattern and interest module

New RDA contracts can be created through a factory contract which serves as a registry. Users can find all contracts involved with a specific address.

The factory contract is available on the Ethereum Main Net, the Kovan Test Net and on my personal test net with instant mining.

# Modularity

## Factory-child pattern and interest module

New RDA contracts can be created through a factory contract which serves as a registry. Users can find all contracts involved with a specific address.

The factory contract is available on the Ethereum Main Net, the Kovan Test Net and on my personal test net with instant mining.

The DSR saving contract module is separate and can be replaced by a module that invests the deposit differently.



# Overview

## The Problem

- The zero-interest problem
- Smart contracts and stablecoins
- How to invest the deposit

## The Smart Contract

- A graphical overview
- Multisig
- Documents
- Modularity
- Security and testing**

## The Off-Chain Contract

- Legal document

## The Interface

- smartdepos.it

## The Future

- What needs to be done
- Use case for the contract

# Security

## Security by design

Every function is either internal, view or pure or requires a sender address from a participant. No account other than the three hardcoded participants can change the contract state.

# Security

## Security by design

Every function is either internal, view or pure or requires a sender address from a participant. No account other than the three hardcoded participants can change the contract state.

No dependencies on libraries or other contracts except for the MakerDAO system.

# Security

## Security by design

Every function is either internal, view or pure or requires a sender address from a participant. No account other than the three hardcoded participants can change the contract state.

No dependencies on libraries or other contracts except for the MakerDAO system.

Migrate allows the participants to rescue the funds in case of an emergency or invalid state and allows for a controlled transfer to an updated contract.

# Security

## Security by design

Every function is either internal, view or pure or requires a sender address from a participant. No account other than the three hardcoded participants can change the contract state.

No dependencies on libraries or other contracts except for the MakerDAO system.

Migrate allows the participants to rescue the funds in case of an emergency or invalid state and allows for a controlled transfer to an updated contract.

Extensive truffle test suite with dozens of unit-, integration- and story driven tests.

# Overview

## The Problem

- The zero-interest problem
- Smart contracts and stablecoins
- How to invest the deposit

## The Smart Contract

- A graphical overview
- Multisig
- Documents
- Modularity
- Security and testing

## The Off-Chain Contract

- Legal document**

## The Interface

- smartdepos.it

## The Future

- What needs to be done
- Use case for the contract

# Regulations

An accompanying legal document

In collaboration with a jurist, we are in the process of composing a Swiss legal document (in German) that specifies the rights, obligations and distribution of risks among the participants involved in a smart rental deposit account contract.

# Regulations

An accompanying legal document

In collaboration with a jurist, we are in the process of composing a Swiss legal document (in German) that specifies the rights, obligations and distribution of risks among the participants involved in a smart rental deposit account contract.

It regulates, among other things:

- ▶ Safekeeping of private keys
- ▶ Representation through other parties



# Regulations

An accompanying legal document

In collaboration with a jurist, we are in the process of composing a Swiss legal document (in German) that specifies the rights, obligations and distribution of risks among the participants involved in a smart rental deposit account contract.

It regulates, among other things:

- ▶ Safekeeping of private keys
- ▶ Representation through other parties
- ▶ Distribution of transaction costs and fees
- ▶ Reasons for migrations

# Regulations

An accompanying legal document

In collaboration with a jurist, we are in the process of composing a Swiss legal document (in German) that specifies the rights, obligations and distribution of risks among the participants involved in a smart rental deposit account contract.

It regulates, among other things:

- ▶ Safekeeping of private keys
- ▶ Representation through other parties
- ▶ Distribution of transaction costs and fees
- ▶ Reasons for migrations
- ▶ Tax declaration of interest profits

# Overview

## The Problem

- The zero-interest problem
- Smart contracts and stablecoins
- How to invest the deposit

## The Smart Contract

- A graphical overview
- Multisig
- Documents
- Modularity
- Security and testing

## The Off-Chain Contract

- Legal document

## The Interface

- smartdepos.it**

## The Future

- What needs to be done
- Use case for the contract

A powerful dApp is provided to interact with the RDA:

`https://smartdepos.it`

A powerful dApp is provided to interact with the RDA:

`https://smartdepos.it`

It offers:

- ▶ Managing your involved RDAs

A powerful dApp is provided to interact with the RDA:

`https://smartdepos.it`

It offers:

- ▶ Managing your involved RDAs
- ▶ Metamask integration

A powerful dApp is provided to interact with the RDA:

`https://smartdepos.it`

It offers:

- ▶ Managing your involved RDAs
- ▶ Metamask integration
- ▶ State of the art technology: React, node, web3.js

A powerful dApp is provided to interact with the RDA:

<https://smartdepos.it>

It offers:

- ▶ Managing your involved RDAs
- ▶ Metamask integration
- ▶ State of the art technology: React, node, web3.js
- ▶ Pure front-end dApp, blockchain is the only source of truth



A powerful dApp is provided to interact with the RDA:

`https://smartdepos.it`

It offers:

- ▶ Managing your involved RDAs
- ▶ Metamask integration
- ▶ State of the art technology: React, node, web3.js
- ▶ Pure front-end dApp, blockchain is the only source of truth
- ▶ Open source

# Overview

## The Problem

- The zero-interest problem
- Smart contracts and stablecoins
- How to invest the deposit

## The Smart Contract

- A graphical overview
- Multisig
- Documents
- Modularity
- Security and testing

## The Off-Chain Contract

- Legal document

## The Interface

- `smartdepos.it`

## The Future

- What needs to be done
- Use case for the contract

# What needs to be done

Polish and legal formalities

Well ahead of the schedule for the hand-in date.

Contract testing on Kovan and Main Net mostly completed.

# What needs to be done

## Polish and legal formalities

Well ahead of the schedule for the hand-in date.

Contract testing on Kovan and Main Net mostly completed.

This leaves enough time to

- ▶ Polish and check legality of off-chain contract

# What needs to be done

## Polish and legal formalities

Well ahead of the schedule for the hand-in date.

Contract testing on Kovan and Main Net mostly completed.

This leaves enough time to

- ▶ Polish and check legality of off-chain contract
- ▶ Incorporate feedback

# What needs to be done

## Polish and legal formalities

Well ahead of the schedule for the hand-in date.

Contract testing on Kovan and Main Net mostly completed.

This leaves enough time to

- ▶ Polish and check legality of off-chain contract
- ▶ Incorporate feedback
- ▶ Finish written thesis

# Overview

## The Problem

- The zero-interest problem
- Smart contracts and stablecoins
- How to invest the deposit

## The Smart Contract

- A graphical overview
- Multisig
- Documents
- Modularity
- Security and testing

## The Off-Chain Contract

- Legal document

## The Interface

- `smartdepos.it`

## The Future

- What needs to be done
- Use case for the contract

# Use case for the contract I

## Use in a rental contract

During April 2020 I was in the process of moving to a new house. After discussing my seminar thesis with the new landlord, my new flat mates and the jurist consultant we decided to move ahead and included the following section in the rental contract:



# Use case for the contract I

## Use in a rental contract

During April 2020 I was in the process of moving to a new house. After discussing my seminar thesis with the new landlord, my new flat mates and the jurist consultant we decided to move ahead and included the following section in the rental contract:

*Das Mietzinsdepot wird im gegenseitigen Einverständnis unter Einbezug eines Treuhänders in einem auf der Ethereum Blockchain bereitgestellten Smart Contract hinterlegt.  
[...]*

# Use case for the contract II

## Use in a rental contract

*Die Einzahlung in den Smart Contract erfolgt in einem an den US-Dollar gebundenen Stablecoin zu dem zum Einzahlungszeitpunkt geltenden Wechselkurs. Änderungen im Wechselkurs zwischen Schweizer Franken (CHF) und dem Stablecoin werden von Vermieter und Mieter in Kauf genommen und haben keine Anpassung der Höhe des Mietzinsdepots zur Folge. Weitere Vereinbarungen betreffend des Smart Contracts sind im Dokument Nutzungsbestimmungen für einen Smart Rental Deposit Account schriftlich festgehalten und gelten als Bestandteil des Mietvertrags.*

# Thanks!

Q & A

I will be happy to show you a smart rental deposit account contract in action and answer your questions!

Github: <https://github.com/matnad/rental-deposit-account>

# References



GNOSIS, [gnosis/multisigwallet: Allows multiple parties to agree on transactions before execution](#), 2019.



Fabian Schär, [Decentralized finance: On blockchain- and smart contract-based financial markets](#), preprint, 03 2020.