Hackathon*Hamburg

Table of contents

Team

Dr. Anika Patz

Niels Launert

Ibo Sy

Lukas Cremer

Malte Giere

Frank Jungbeck

Arnab Naskar

Assumptions

- Bearer bonds (‘**Securities**’) which can be issued/transferred to only identified investors by the Company (‘**Issuer**’).
- The Securities are issued on the Ethereum blockchain as an ERC-20 compliant standard token. Such tokens are termed as ‘Securities Token’.
- The Securities Token (‘**Token**’) represent the ownership of a claim on the Ethereum blockchain.
- Company name- tbd; Token name- MCART (*Most Compliant and Regulated Token*).
- Tokens are issued under German law.
- Maximum number of Tokens to be issued by the Issuer: 50,000,000.
- Price of the Token: 1 Token = 1 Euro.
- The Issuer controls the Smart Contract through a multi-signature process.
- We are assuming an Euro stable coin is being used by the Investor.
- Tokens are only issued as Euro stable coin is paid by the Investor.

Deployment of the Smart Contract for Tokens

The smart contract manages the relationship between the Issuer and the investors. The smart contract aims to reflect certain rights and obligations between the parties.

Srl. no.	Feature description- Basic (Implemented)	Feature description- Resource heavy	Feature description- impossible
1.	No more than 50,000,000 Tokens can be issued by the Issuer through the Smart Contract.		
2.	The identity of the prospectus document can be referenced on the Blockchain. The .pdf can be stored in the database (IPFS) and can be hashed.	The document can be also updated and the hash can be updated with traceability.	

Issuance and Subscription of the Smart Contract for Tokens

In this part the Tokens are bought by the investors via the subscription agreement and the investor receives the tokens after the payment has been made to the Issuer.

Srl. no.	Feature description- Basic (Implemented)	Feature description- Resource heavy	Feature description- Impossible
1.	Investors pay with Euro stable coin	Ether and other cryptocurrencies along with Euro route.	
2.	Investors have 14 days to revoke the investment amount Investors can call the revoke function via a provided interface via enabling a button “I herewith declare my right of revocation”. This will trigger retransfer to the Issuer/burning (retraction) of Tokens and the Euro stable coin will be refunded.	Investors get paid back after 3% is deducted.	
3.	Investors have to whitelist before they receive Tokens. Only investors from Germany can invest.		
4.	Enabled mint function. Tokens are only issued once the Euro stable coin is paid.		
5.	Tokens can be hold by the investor in any ERC 20 compatible wallets.		
6.	Initial subscription restriction - min. of 1000 Tokens	Different category of investors can have different subscription cap restrictions.	

Transfer between Investors

In this part we will discuss how the Tokens can be transferred between the investors without a DVP in place.

Srl. no.	Feature description- Basic (Implemented)	Feature description- Resource heavy	Feature description- not practical on blockchain
1.	Investors can be added to the whitelist by the Issuer, subsequent to the issuance of the Tokens. Investors can only hold tokens once they are whitelisted. The smart contract contains a function that restraints a Token holder from transferring their Tokens to a non-whitelisted investor. One option can be that the investors can transfer the token without KYC but in such situation the subsequent investor cannot hold the full rights of the bearer. In such situation there is the risk that the subsequent investor fails KYC. High compliance risk.		
2.	Transfer of Tokens will transfer the interest rights and the voting rights.		
3.	Investors can transfer fractions of the Tokens.		

Payouts

In this part the process and the way how the payouts will be issued to the Investors is discussed.

Srl. no.	Feature description- Basic (Implemented)	Feature description- Resource heavy	Feature description- not practical on blockchain
1.		Timestamp basis: Payouts can only be made to the Token holders/Investors without taking into consideration the time of the holding. Snapshot of Blockchain status on the interest payout day. Calculations of taxes by the Issuer can provide added complexity. In case the Issuer has not got enough liquidity IoU tokens can be issued. Pro-rata basis: Payouts can be made to the Token holders/Investors on quarterly basis based on the pro-rata holding.	
2.		Investors can claim the payouts from the Smart Contract in Euro Stable coins. Payouts in Euro and other cryptocurrencies.	

Voting

In this part the process and the way how voting will be executed is discussed.

Srl. no.	Feature description- Basic (Implemented)	Feature description- Resource heavy/	Feature description- not practical on blockchain
1.		Investors can propose a change/vote (5% of investors minimum). Investors can vote on the change of a contractual term.	
2.		In case the investors participate in a voting and transfer the Tokens, the subsequent token holder may have the following option: 1. cannot vote again - options non-fungible tokens, voting tokens connected with main token etc 2. take a snapshot and restrict the voting rights of the subsequent holder.	

Data Privacy

In this part the process and the way how GDPR requirements are tackled is described.

Srl. no.	Feature description- Basic (Implemented)	Feature description- Resource heavy	Feature description- not practical on blockchain
1.	Investors give consent to be whitelisted on the interface by clicking ‘i hereby give my consent’. Investors can request to de-list from the whitelist. The KYC information of the investor is stored off-chain. Whitelisting is done on-chain		The information of the public key cannot be removed from the blockchain.

Token recovery

In this part the process for Token recovery is described. The Token recovery process allows the force-transfer of tokens.

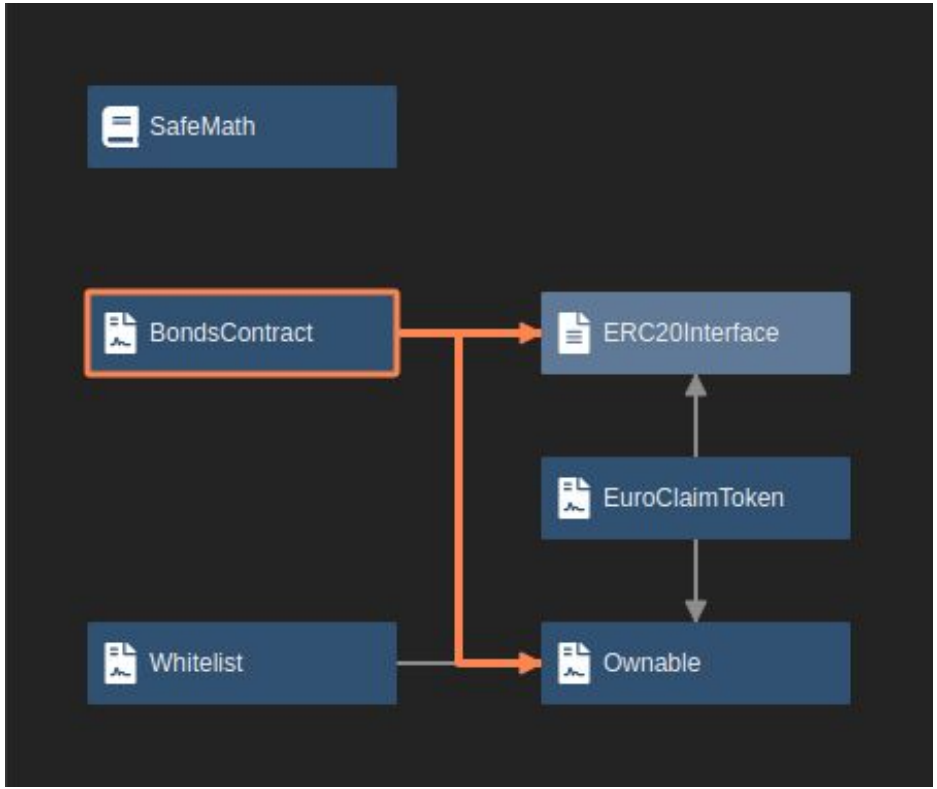
Srl. no.	Feature description- Basic (Implemented)	Feature description- Resource heavy	Feature description- not practical on blockchain
1.	The superuser keys can transfer Tokens from a user to another or burn them through force transfer function. In case the investor loses the Token, they can ask for Token recovery. The force transfer process can be used to restrict the Token access for the investor in case of any legal decision.		

Termination/ Updating of the Smart Contract

In this part the process for termination of the smart contract is described.

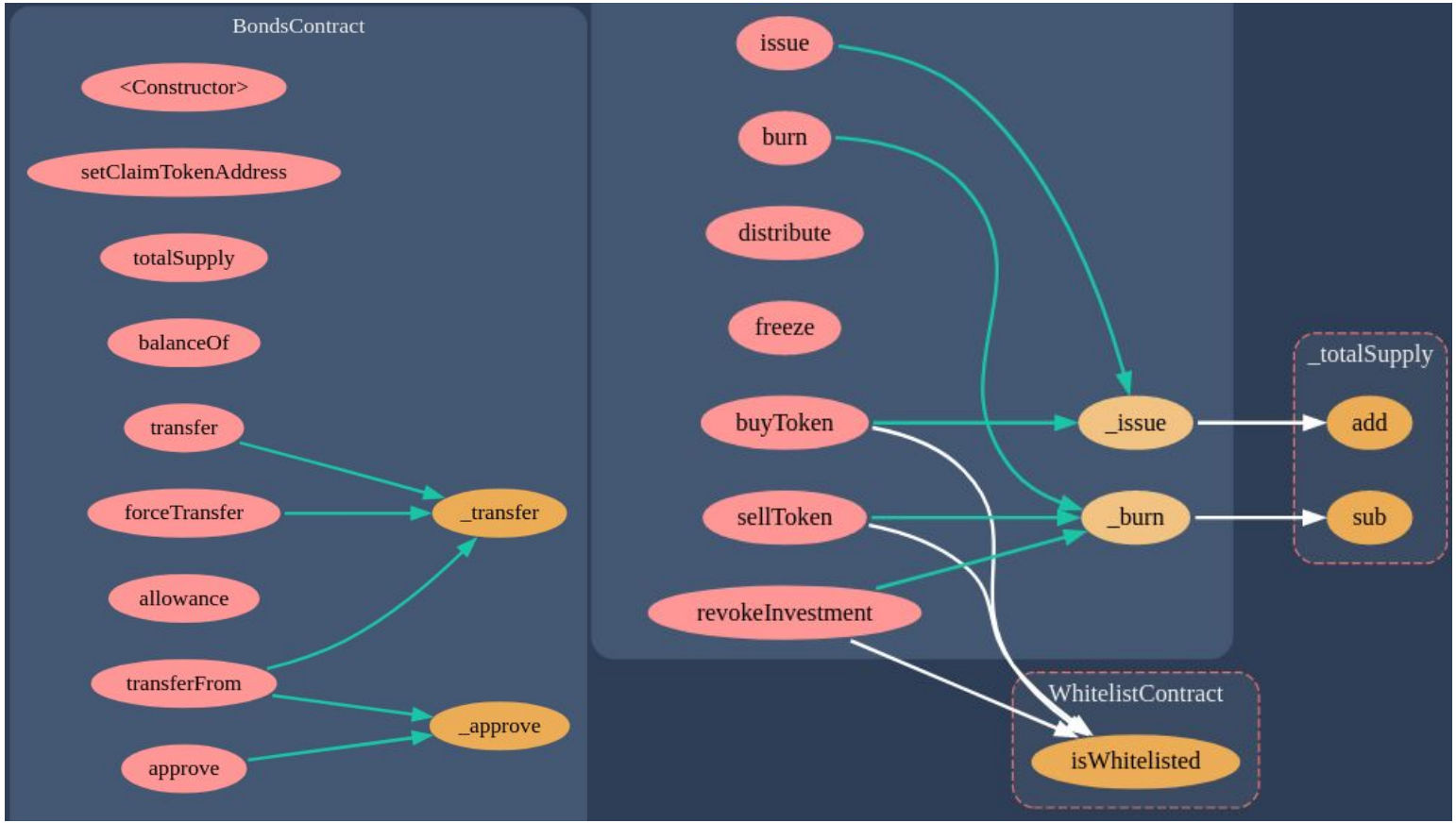
Srl. no.	Feature description- Basic (Implemented)	Feature description- Resource heavy	Feature description- not practical on blockchain
1.	The smart contract is pausable (freezable) that means the Investors can be restricted to transfer any Tokens at any time.		Deletion of the smart contract does not make any sense. Pausing the smart contract may be sufficient enough as the smart contract won't be interactable anymore
2.		After 10 years the Smart Contract can be freezed.	
3.		The Smart Contract can be updated.	

Smart contract architecture



by https://piet.slock.it

Smart contract architecture



Major Challenges

- **Voting**: A voting system would be a complex construction considered Tokens can’t get frozen as long as their voting weight is used in the voting process. Possible to be solved with a snapshot at the time of the vote start though, but too resource-heavy for the short given timeframe
- **Confidential transactions**: Private transactions are possible, but extremely complex and in an experimental state currently.
- **TX costs paid by issuer**: Possible with more time. In Ethereum to make any transaction investors need to pay the Gas fee in Ether. The same can be paid via an ERC-20 token also. For that the Issuer need to pay the gas fee.
- **Pay taxes on-chain**: At least given the German legislation this is an extremely difficult task, since you would need to collect investor-individually church taxes too. It is preferable to do the same off-chain.
- **Standardisation of the terms of the Smart Contract**: Shall we say ‘mint’ or ‘issue’? Shall we say ‘burn’ or ‘retract’?

I am the new smart transfer agent...

```
function _transfer(address sender, address recipient, uint256 amount) internal {
    require(sender != address(0), "ERC20: transfer from the zero address");
    require(recipient != address(0), "ERC20: transfer to the zero address");
    require(!frozen);
    _balances[sender] = _balances[sender].sub(amount, "ERC20: transfer amount exceeds balance");
    _balances[recipient] = _balances[recipient].add(amount);
    emit Transfer(sender, recipient, amount);
}
```

REQUIREMENTS:

MUST use an ERC-20 compatible token for your STO
MUST be able to perform forced transfers for legal actions
MUST use an on-chain whitelist for investors
MUST enable to mint/burn tokens
MUST offer an on-chain solution to purchase (and sell back) tokens
MUST allow the possibility to be executed only through a specific interface (no implementation required)

BONUS: Attach the prospectus document as a .pdf to the token contract

LIMITS: (OFFCHAIN) Only investors from Germany are allowed to invest (KYC)

You are not allowed to raise more than 50,000,000 € (= 50,000,000 token)
Minimal buy-in is 1000 tokens (only relevant for initial buy)

INVESTORS:

There are 200 investors. Each of them wants to purchase 1000 tokens. The investors will use ETH (or a stablecoin) to purchase your token. All of this should work on-chain (you are allowed to use oracles).
Once you bougt your tokens you have 14 days for a withdrawal. An investor decides to return his/her token after 2 days of keeping them. (Rest to be completed.)
An investor wants to sell 50% of its token to a new investor that is not a token holder yet.
An investor wants to sell 20% of its stack to another investor that is a token holder.
An investor was forced to initiate a transaction. Burn the old tokens and mint new ones for the new address. Revert (this can be a mint/burn or a transfer) all transactions (hint: all deadlines stay the same (e.g. payout for interests)).
A token holder has to pay all of his tokens to another investor (court order), but s/he resists/can't to sign the transaction. Enforce the transaction.
An investor duly terminates the term and tries to sell his/her tokens after that to another token holder.
An investor wants to buy more tokens than the maximal limit.
An investor wants to buy only 500 tokens but must buy at least 1000 tokens.
An Investor tries to sell tokens but is not allowed to do so before holding it X days (these days should be a variable that you can update). Asset freezing.

ISSUER:

The issuer mints/burns tokens based on the investments.

MISC:

Extraordinary termination. Your company must face insolvency. Make a public announcement on the blockchain. (Could be also something else the main point is to do public signaling. This could be used for different cases.)

https://github.com/Distributed-Ledger-Consulting/TBD-MCART/blob/master/readme.md