**Royal Grow**

The problem we are going to solve:

The problem of scalability as well as the cost of transactions on the Ethereum blockchain and similar blockchains that support EVM, especially for very small payments. Also, solving the problem of hacking (or exit scam) in all kinds of financial products that are custodial. While this solution is useful in itself, it can still be used as building block for other financial instruments.

Our solution:

Using a smart contract in such a way that only the proof of ownership of the asset(s) is recorded on the blockchain frequently (say every 5 minute). At the same time, everyone can verify his ownership document (and the others too) on the blockchain without spending any money. while the asset owners can withdraw their coins from the contract and transfer them to their own account if they wish (by paying the transaction fee) instantly and unconditionally.

Business opportunity to grow the plan:

Since this project provides a cost-effective, secure and reliable semi-custodial infrastructure for storing and transferring coins on the Ethereum blockchain (and blockchains that have similar EVMs), this infrastructure can be used to build other financial instruments (for All ERC20 coins) used.

Probably the most important tool that can be built is the exchange where people can safely buy cryptocurrency in small amounts and not worry about being scammed by the exchange.

Of course, the rest of the financial instruments can be built and developed on the same platform. including all types of bridges, lending platforms and liquidity pools to crowdsourcing plans and selling subscriptions and micro-shares to other functional DAOs.

What is our product:

A smart contract on the Ethereum blockchain, supported by a web3 website and a suitable backend, provides people with an enjoyable experience of buying and transferring crypto and decentralized financial operations.

Our team:

At the moment, it's just me and this is the repository address of the project demo.

<https://github.com/estainit/royal-grow>

Competitors and our difference from them:

The idea of ​​this plan is almost the same as the idea of ​​payment channels (in Bitcoin and Ethereum). With the difference that in our plan it is possible to transfer money between several people and not just one channel between two people or n channels between n couples, which will be routed between them later. Which is very suboptimal and ends up being a kind of game rather than a real payment path.

In our plan, in addition to the implementation of the infrastructure for storing and transferring coins, many incentives are also considered for involving people in the protocol, providing liquidity, and even playing the role of an oracle, all of which together provide a dynamic and growing ecosystem.

Financing and project costs:

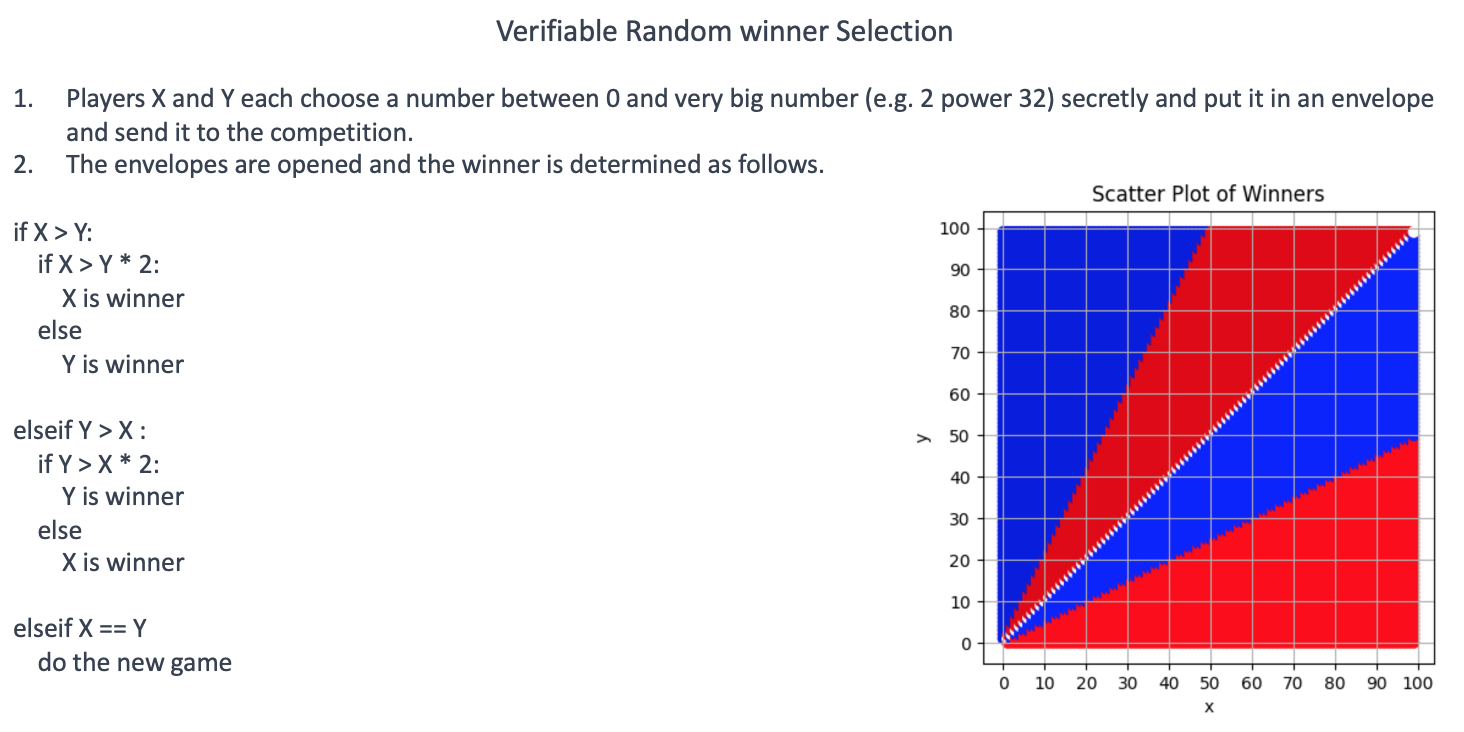
More important than financing the project is forming a network of people in the cryptocurrency ecosystem and advertising for the final product. Therefore, regardless of the costs of creating and developing the product (writing the smart contract and Audit and its security inspections, front and back design and relevant tests), the most important cost will be related to branding and explaining and explaining the product and gaining the confidence of the people and of course the specialists of this The area about system security and the safety of users' assets. My suggestion for the product is an open-source license (preferably GPL 3) so that the code of all three front and back parts and the smart contract can be viewed, reviewed and changed by everyone. Our source of income will be from our own customers. While anyone can use our code or improve it and use it for their business and even replicate the entire ecosystem. In any case, since we were the original and original provider, and we also have a complete road map for its development, copies do not have much chance of success.

Ways to earn money:

The main source of income for the system is receiving money transfer fees. For example, customer number one requests the transfer of money to customer number two and asks us (as a company) to produce the document of ownership of the money for the second customer (in fact, to give a commitment that the customer, by presenting it on the network, can unconditionally and the condition is that he withdraws money from the contract and transfers it to his own account or transfers it to another person in the same ecosystem.) and also reduce the amount demanded by the first customer. We ask the sender for some ether (worth a few cents) as a fee to perform this operation.

A percentage of this income is sent to the Oracle Fund, and at the same time as the money transfer operation is carried out, we ask the money sender to help us (if desired) in providing important information (equal price of currencies, metals, and stocks) and in return, the chance of this to win some ether from the Oracle fund.

The lottery operation and determining the winner of the Oracle Fund has two stages. First, select a number of participants randomly (verifiable random algorithm that I wrote myself and can be accessed at https://github.com/estainit/verittery)



And in the second stage, sorting the winners based on the information provided and finally choosing the middle of the information and the person providing it as the winner.

Another source of income is the DCMR tax collection system. Consider a situation where we are not the only company in the contract and other companies (just like us) issue ownership documents for a number of coins by taking fiat or services from people. These documents are combined and form a Merkel tree, and the root of the Merkel tree (DCMR) is regularly (for example, every five minutes) stored on the blockchain (only the hash of the root of the Merkel tree), and each company is responsible for this storage. deposit an amount to the contract treasury and this treasury is distributed among the project stakeholders in regular periods.

To be a shareholder of the project, you must have some Ether in the contract and this amount remains untouched for a week. With a difficulty adjustment algorithm, we can calculate this amount so that no more than 100 new shares are produced per week. At the beginning, our company has, for example, a thousand shares, and every week 100 new shares are produced and added to the existing shares. Now, every person who owns the shares of the system receives a share of the DCMR tax according to the amount of his share.

Any identity can be a shareholder and it does not have to be a company.

This subsystem and its stakeholders can be used for DAO and other contract governance issues.

Some technical details:

We have two basic factors in the system

Agent or company: We are the ones who have provided the infrastructure of the system.

Creditor or customer: are system users who buy cryptocurrency from us in exchange for paying fiat money (or performing services). Customers can also transfer crypto among themselves.

Still, these prerequisites and requirements must be maintained in the system.

- The company cannot put a cap on customers in any way.

- Whenever the customer wants, he can withdraw his coins from the contract as soon as possible and transfer them to his account.

- Using the system for the customer should be easy, fast and economical.

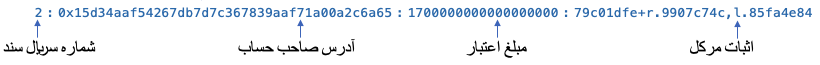
The two main operations of the system are the initial charge of the account and the transfer of funds.

.

Initial deposit 

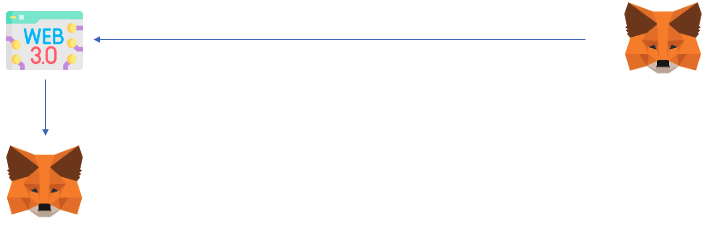
1. The user connects his wallet to our site and then sends an amount of Ether to the contract address.

2. As soon as the user pays this amount, he will see a receipt on the website that he can copy and save in a safe place and use this document whenever he wants to withdraw his money from the contract. Obviously, during the next transactions, the customer's balance will change, and for this reason, a new receipt will be presented to the customer, and the previous receipts (with a lower serial number) will be invalidated. The submitted document will have the following format.



Note: In normal mode (that is, when the company is honest), the user does not need this receipt and always has complete control over his coins. This receipt is issued only when there is a dispute between the company and the customer.

Fund transfer



1. The user signs the token transfer request through his wallet connected to our site and sends it to our bank.

2. After completing all the security checks, we create 2 new receipts and store them in the database. We provide an updated receipt for the sender and a new receipt for the recipient and both to the sender. Now, by seeing both documents, the sender is sure that the transfer has been done correctly. The sender can give the second document directly to the recipient or ask the recipient to connect to our site (with the address mentioned in the document) and download the document.

In the following, I need to explain a little about DCMR and how to store it on the blockchain. As we know, a company may perform millions of off-chain transactions and finally calculate the balance status of all accounts in the form of a Merkel tree and calculate the Merkel root of that tree and store it like that. This root is pushed to the end of a permanent array that is stored on the blockchain, and in this way we always have a record of DCMR on the blockchain and this record is not deleted. On the other hand, the values ​​of the leaves of this Merkel tree and its proofs are transparent and accessible to everyone on the site. In this way, anyone (any customer) by seeing the record related to their request and the relevant proof, can be sure that their request is mentioned in the DC document, and on the other hand, by collecting the sum of all the requests, they can make sure that the company did not sell empty. In fact, each company can issue up to 95% of the balance in the debt document contract, and the remaining five percent is always as a reserve that if the company makes a fake document, the first person who reports this fraud will receive this 5% as a reward. .

In general, in such a system, the most important issue is that the company cannot cheat. Otherwise, the customer (who is dependent on the company for any type of transfer) cannot do much. If we can prevent the fraud of the company, we have indirectly prevented the hacking of the system (common hacking of exchanges, which are usually done by leaking private keys or discovering loopholes in payment operations).

For this purpose, we have limited the possibility of withdrawing money from the contract to the existence of a "credit proof document" and only in this way can the funds in the contract be withdrawn. Even the management of the company and Owner Contract cannot withdraw any money from the contract!

The scenario that comes to mind is that the owner of the company can't register a corrupted DCMR document on the blockchain, whereby he can take all the resources himself? The answer to this assumption is yes, but there are additional conditions that make this action impossible. In this way, after updating the DCMR (which happens, for example, every five minutes), withdrawal from the contract is locked for two minutes, and withdrawal requests are sent to a waiting queue, which can be withdrawn in order of receipt after the lock is removed. But in these two minutes, if someone has a claim against the new DCMR and that his claim is not mentioned in this document and accompanying proofs, he can block the collection in general (and for everyone) so that the status of his claim is checked. And if the customer's claim is true, the last DCMR is dropped from the validity level and the last one (and the previous ones) are valid.

The first person to file a bug report will also receive a reward for announcing it, which will make him not only take care of his funds, but also do a quick test on all available funds, or even set up services that, by taking money from customers, Take over the job of protecting their money.

weak points:

Yes, our website should be up and running 100% of the time like a classic website and provide services, and it does not have claims like Bitcoin in this regard. In addition, all cryptocurrencies (except Bitcoin) are dependent on third-party sites that provide blockchain connection services, and their claim of decentralization is just a gimmick.

Yes, our site can censor transactions and block some addresses from serving, as currently all cryptocurrencies have this restriction, and only Bitcoin is an exception to this rule to some extent.

Yes, this app doesn't do much in terms of increasing user privacy, although it is likely that future developments will improve it with newer technologies such as zero-knowledge proofing.