Confido

Whitepaper v0.2

INHOUD

EXECUTIVE SUMMARY

This white paper provides a detailed look at the new payment solution called Confido. Confido is a payment solution developed to be used by both businesses and individuals. It provides secure escrow payments using smart contracts, without relying on a third party to control the money. The unique thing about Confido is its shipment tracking feature. Confido will track a package up to the point that it gets delivered, and will only then release the funds. This is all done in a trustless and decentralised fashion using smart contracts on the Ethereum and RSK blockchain. In case of a faulty or wrong product the buyer can put the transaction on hold and resolve the issue with the seller through our messaging system.

Confido takes away the trust barrier in exchanges involving cryptocurrencies, while also staying decentralised and trustless. For example, when a person (the buyer) wants to buy a keyboard from someone (the seller) with cryptocurrency, he'll have to trust the seller. The seller can run away with the funds and never send anything, there are no identities attached to a Bitcoin or Ethereum address. Confido takes away this trust barrier by providing a secure escrow payment solution which is trustless, decentralised and open-source.

There is a 0.7% transaction fee when using Confido. This is very low in comparison to other escrow services. As of now Bitcoin and Ethereum are accepted forms of payment. In the future we will add more cryptocurrencies.

The token that will be sold in the ICO is called the Confido token. The Confido token is a basic ERC20 token that has the same capabilities as most other ERC20 coins. The thing that makes Confido tokens valuable is the ability to earn Ether passively by holding tokens. Users that have invested in Confido tokens will receive 0.7% in ETH of the payments made through Confido (they will receive 100% of the transaction fees paid by the users). That means that investors will earn money simply by holding the token. Pay-outs are bimonthly and will start in Q2 2018. The Confido token can also be used as a form of payment on the Confido platform. It will be the only fee-less currency on our platform.

The hard cap of our ICO is $500,000. Fifteen million tokens are in existence, of which 12,000,000 will be sold during our ICO, 750,000 will be set aside for our bounty campaign and 2,250,000 (15%) will be held by the company. Our hard cap is so low because we want to start with a low market cap to ensure greater growth potential for our investors. We really appreciate our initial investors, because they were the first to put their money and trust in us. Therefore, we want to maximise returns for them. Another reason for the low market cap is that we are not some money-grabbing company that wants to raise millions through an ICO without a fully functioning product and/or existing customers.

The collected funds will be used for product development, marketing and legal fees. Unsold tokens will be burned.

INTRODUCTION

Cryptocurrency is new, exciting technology. Every day more and more people are getting into cryptocurrencies; it's quickly gaining steam. If you're reading this you're probably interested in cryptocurrency yourself, but have you ever tried to purchase anything with it? If you have, then you've most likely experienced the anxiety when sending a payment to a stranger.

There is a big trust barrier when dealing with cryptocurrency. It's so easy to scam with, because there are no identities attached to a wallet address. Therefore, a lot of people refrain from using cryptocurrency in peer to peer transactions/exchanges.

There are some solutions, but they are centralised and require the user to trust a third party, which kind of defeats the purpose of cryptocurrency. Cryptocurrency should be trustless and decentralised.

THE PROBLEM

Cryptocurrency is a booming market. Every day more and more people hear about, and interact with, cryptocurrency. The problem with cryptocurrency is that it's anonymous - there is no identity attached to a Bitcoin or Ethereum address. For a lot of use cases that's great, but it's not ideal when exchanging cryptocurrency for digital or physical goods. The anonymity of cryptocurrency makes it an easy target for scammers, they can just run away with the coins without any consequences whatsoever.

The current peer-to-peer exchange of goods for cryptocurrency goes something like this:
We have a buyer, Bob, and a seller, Allie. Allie is selling a cologne she found in her room on a popular second hand website. Bob wants to buy the cologne from Allie. He sends her a message and they agree that Bob can have the cologne for $40. Allie lives pretty far away from Bob, so he decides to just let Allie send him the cologne. Bob sends the payment directly to Allie and expects Allie to send the product to him after she has received the payment.

With the setup above we would have to rely on trust. The buyer has to trust the seller in that he/she will send the product after the payment has been made. The problem with that is that people are naturally very distrusting of other people. Couple that with the fact that there are no identities attached to cryptocurrency wallet addresses, which makes them very easy to scam with, and you've got a serious trust-issue here.

For exchanges between individuals with fiat money there is, for example, PayPal. People use PayPal because it's regarded as a safe payment method. When there is a dispute between a buyer and seller PayPal is there to resolve the issue. The buyer and seller don't have to trust each other when using PayPal, hence why it's so popular. It takes away the trust barrier.

What people don't realise is that behind PayPal there is a big company (PayPal Holdings Inc.) that they have to trust with their money. In our opinion, this is not ideal, since it technically doesn't take away the trust barrier. The user still has to trust PayPal to handle, and hold, their money which sometimes goes very wrong. There are thousands of complaints from innocent people whose account got shut down. A payment method should be secure and trustless.

We came up with a solution for this: Confido.

OUR SOLUTION

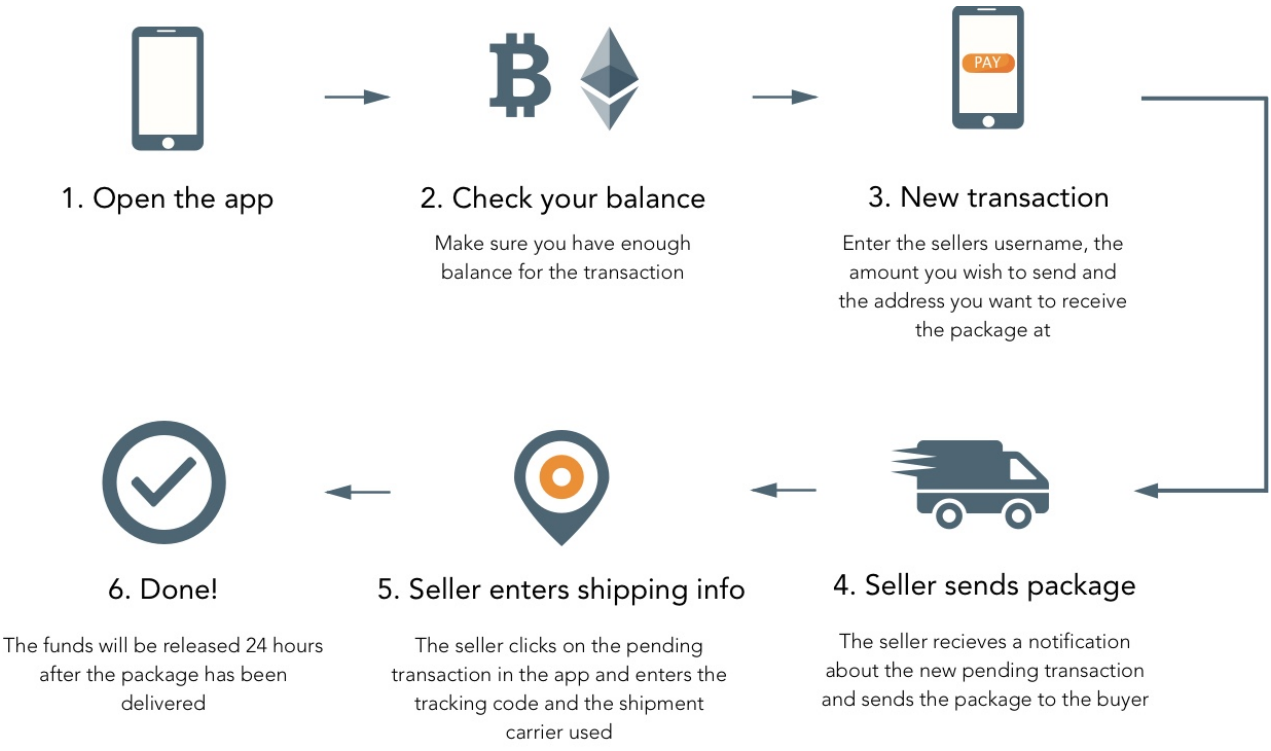
Our solution to the problem described above (see section “The Problem”) is Confido.

What is Confido?

Confido is a payment solution developed to be used by both businesses and individuals. It provides secure escrow payments using smart contracts, without relying on a third party to control the money. The unique thing about Confido is its shipment tracking feature. Confido will track a package up to the point that it gets delivered, and will only then release the funds. This is all done in a decentralised and automated fashion using smart contracts.

How does Confido work?

The way it works is quite simple. Here is how it works for the user(s):



The commercial explanation of Confido

For the more technical readers we have made an infographic of what goes on behind the scenes:

The technical explanation of the process behind Confido

Text explanation:

We utilise Keycloak for secure log-ins and two-factor authentication. Blockchain.info's API will be used to generate a BTC wallet and ETH wallet for new users, which are tied to their Confido username. When a buyer sets up a new transaction all the data entered by the buyer gets encrypted using Oraclize and sent to a newly-generated smart contract. This smart contract will be generated using a pre-made smart contract template. After the smart contract is generated the funds will get send to the smart contract.

After that, it's the sellers turn. Our platform sends a notification to the seller about a new pending transaction. The seller sends the product/package to the buyer. After he has send the package he can click on the pending transaction, enter the shipment tracking code and select the shipping carrier he used. The data gets encrypted using Oraclize and gets sent to the smart contract.
Now it's the smart contracts turn. First, it determines which shipping carrier was used. After that it looks up the shipment tracking code using the API of said shipping carrier to check if the address the package was sent to matches with the address that the buyer entered when setting up the transaction. If the address matches, the smart contract will wait till the status of the package says 'Delivered'. When the status says 'Delivered' a countdown will start and the money will get released after 24 hours.

What if the product sent by the seller is faulty or the wrong product?

In the worst case scenario the buyer can put the transaction on hold. This means that the money is stuck in the smart contract. The buyer only has the option to release the money to the seller, and the seller only has the option to refund the buyer. The buyer and seller will have to resolve their issue and come to a conclusion using our secure messaging system.

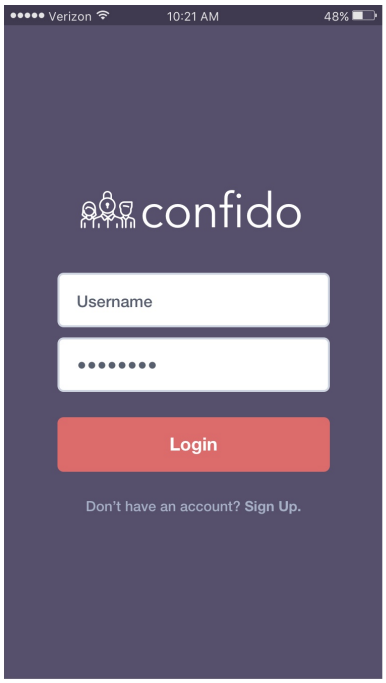
VISION

"Confido aims to be the go-to payment solution for peer-to-peer transactions involving the exchange of a physical product for cryptocurrency. When cryptocurrency hits the mainstream public Confido wants to be the number one choice for peer-to-peer transactions involving physical products. We want to develop a secure way of transacting with other individuals without having to trust them.

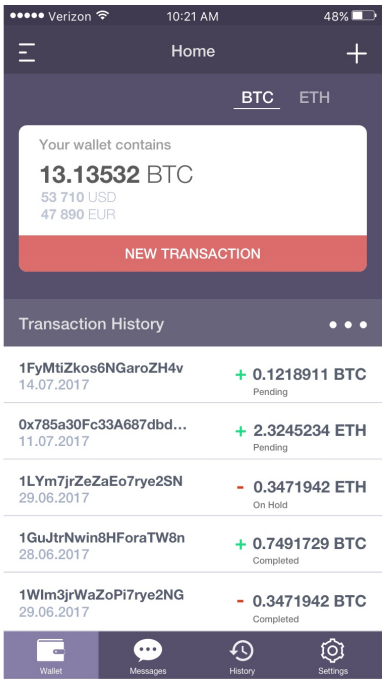
Confido will become a household name on sites like Craigslist and Oodle. Users will choose to pay with cryptocurrency instead of the old school fiat money.

Our payment solution will cater to both individuals and businesses by providing individuals with an easy-to-use app and businesses with a secure and easy to integrate API."

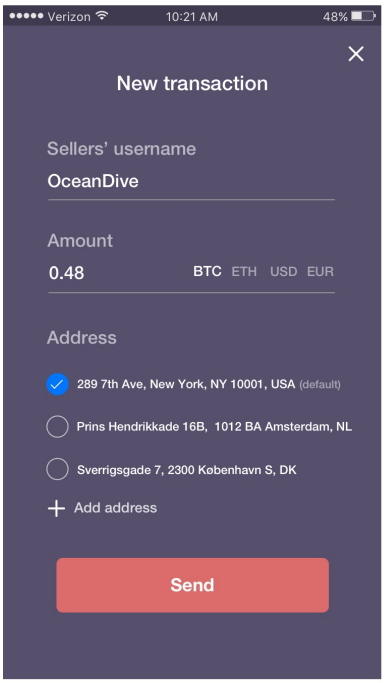
PROJECT OVERVIEW



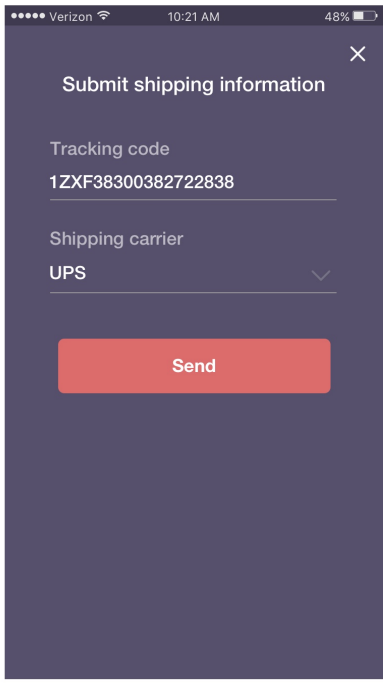
The login screen. You can login if you already have an account, or you can register by clicking on "Sign Up" under the login button.



The dashboard/home screen. Here users can see their balance and their latest transactions. They can also click on the 'New Transaction' button to start a new transaction. By clicking on the little '+' in the top right corner, users can deposit funds into their wallet.

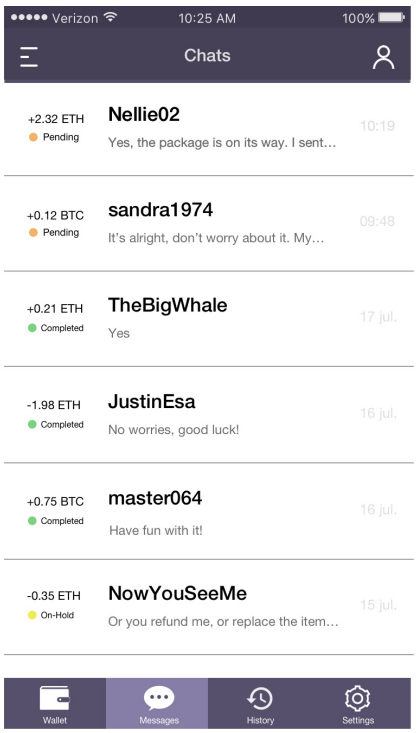


The 'New Transaction screen. This is what users see when they click on 'New Transaction' in the home screen. Users can set up a new transaction here by providing the sellers username, the amount they wist to send and the address they would like to receive the product at.

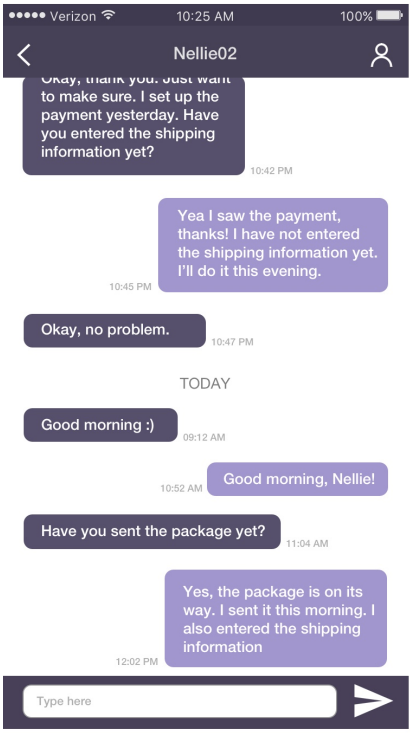


The 'Submit shipping information' screen. This is what users (sellers) see when they click on a pending transaction. Here they can submit the shipping info to the smart contract.

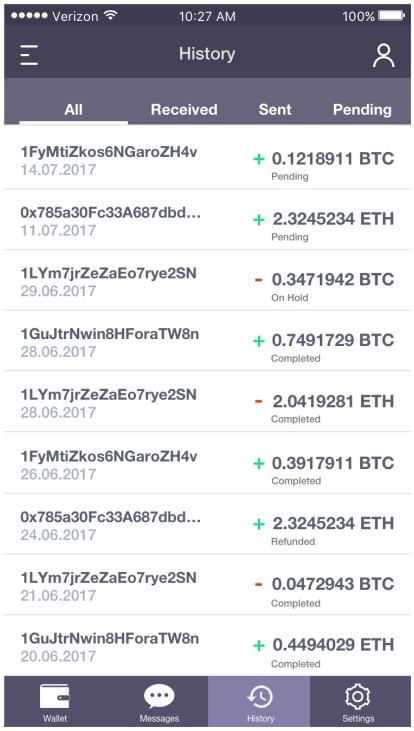
The deposit screen. This is what users see when they click on the little '+' on the top right corner of the home screen. Here they can see their deposit address.



The messages screen. Here users can see all their chats with the sellers/buyers. The transaction info and status is shown on the left, next to the username.



The chat screen. This is what it looks like when users click on a chat. Here the buyer and seller can ask each other questions and keep each other updated.



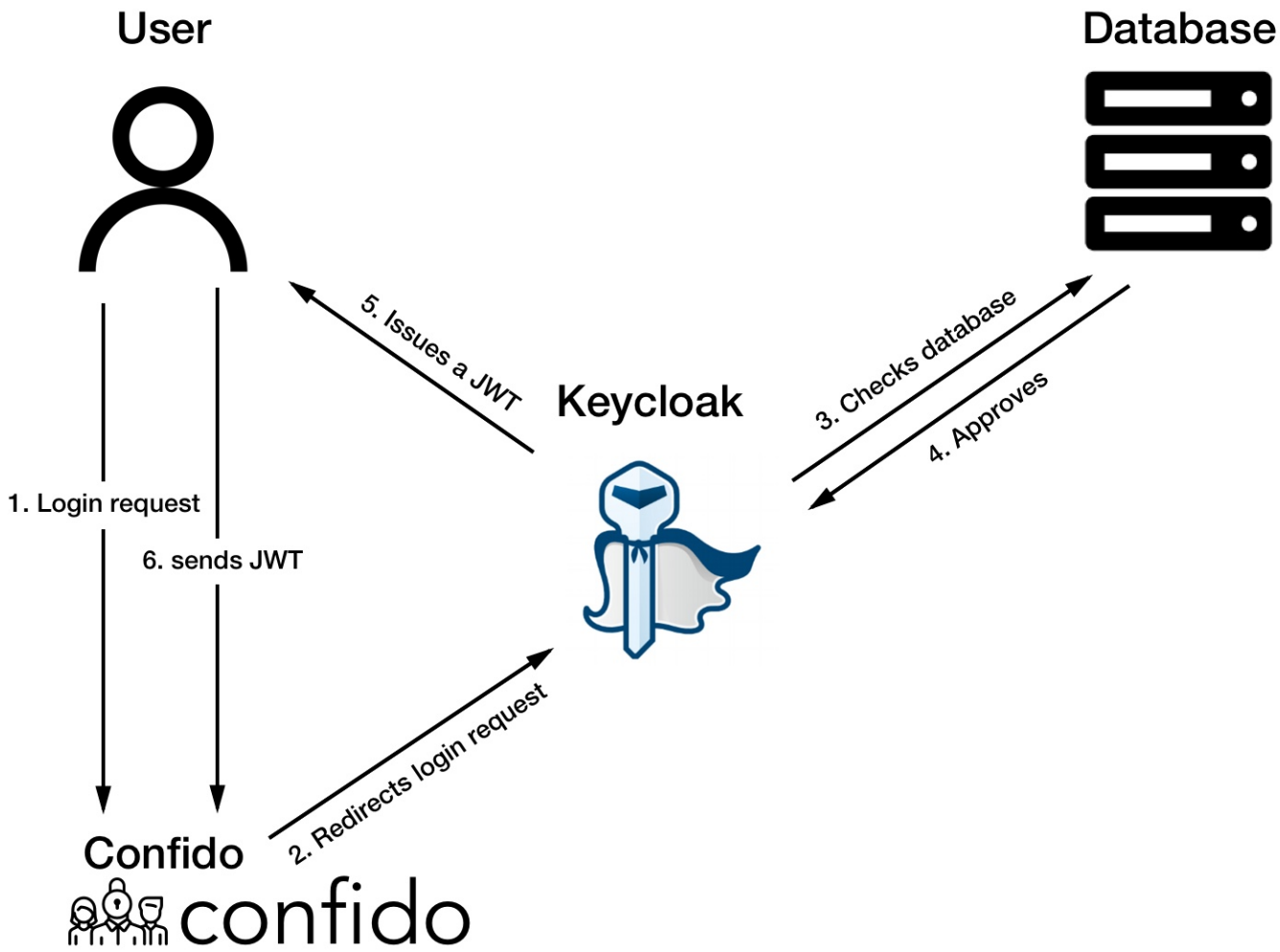
The transaction history screen. Here users can see their past transactions and check their status.

SECURITY

Security is a big issue in the crypto-world. With things like the DAO hack in 2016 and the recent Parity hack users are more concerned about security than ever before. Smart contracts have to be absolutely bug-free.

Log-in and account security

First of all, we will use Keycloak to provide our users with the option to use two-factor authentication. Keycloak is an open source Identity and Access Management solution aimed at modern applications and services. It's based on standard protocols and provides support for OpenID Connect, OAuth 2.0, and SAML. This is how it works:



We will also require authentication via Keycloak before or during any transactions on the platform. This means that users can trust that merely having access to the platform is not enough to transfer value—you must also re-authenticate, thus protecting any value you have stored on the platform.

Smart contract security

We have the advantage of only having one single smart contract template. This template will be tested vigorously to ensure there are no bugs. The smart contract template is built in the latest version available of Solidity. We prefer Solidity over Serpent because it provides the most secure interface for programming on the Ethereum network.

Data sent to the smart contract

All data sent to the contract gets encrypted using Oraclize. The data is safe from prying eyes and can only be decrypted by Oraclize.

THE MARKET

We want to become the go-to choice for peer-to-peer transactions involving a physical product. The market we are going to focus on at first is the apparel resale industry. This might sound like a small market, but don't underestimate the size of it. In 2017 the apparel resale industry was worth a whopping $18 billion. The market is growing rapidly, the whole apparel resale industry is expected to be worth $33 billion by 2021. Millennials are the most likely group to shop secondhand in the future.

USE CASES

Example #1: A normal transaction between individuals

Carl wants to buy a laptop from John. Carl and John do not know each other, but both prefer to use cryptocurrencies. Because of the high price of the laptop, Carl does not feel comfortable by sending the money up-front to John. That's why they decide to use Confido. Carl simply opens the app, checks his balance and then sends the money to John by providing his username, the amount he wants to send and the address where he wants to receive the laptop. After that John gets a notification about a new pending transaction. He sends Carl the laptop and gets a shipment tracking number. John opens the Confido app on his phone, clicks on the pending transaction, enters the shipment tracking number and selects the shipping carrier he used. That's it. The shipment will be tracked by our smart contract and the money will be released 24 hours after the package has been received.

Example #2: A transaction between individuals that goes wrong; the seller sends a faulty product

Ted has bought a brand new stand mixer from Barney using Confido, exciting stuff. Upon arrival Ted unboxes the stand mixer but it seems like it's not working.. Upon further inspection it seems that the mixer Barney sent to Ted is faulty. That's a problem, because the payment will soon be released. Ted decides to put the transaction on hold to resolve the issue with Barney. He opens the Confido app, clicks on the pending transaction and puts it on hold. After that he messages Barney about the faulty product and they work it out over chat; Barney decides to refund Ted. He clicks on the transaction and is met with only one option: Refund the buyer (Ted's only option is to release the funds to the seller). Barney clicks on it and is prompted with a success message. The money instantly gets sent back to Ted.

Example #3: A transaction between an individual and an ecommerce store

Alison wants to buy a cute handmade handbag she saw on an ecommerce store. She adds the handbag to her shopping cart and goes to checkout. At the checkout she selects the option "Pay with escrow", provided by Confido. A smart contract gets generated using the details entered by Alison on the checkout page. She's presented with the address of the smart contract that she can send the money to. She sends the money to the smart contract and is then presented with a thank you for ordering page.

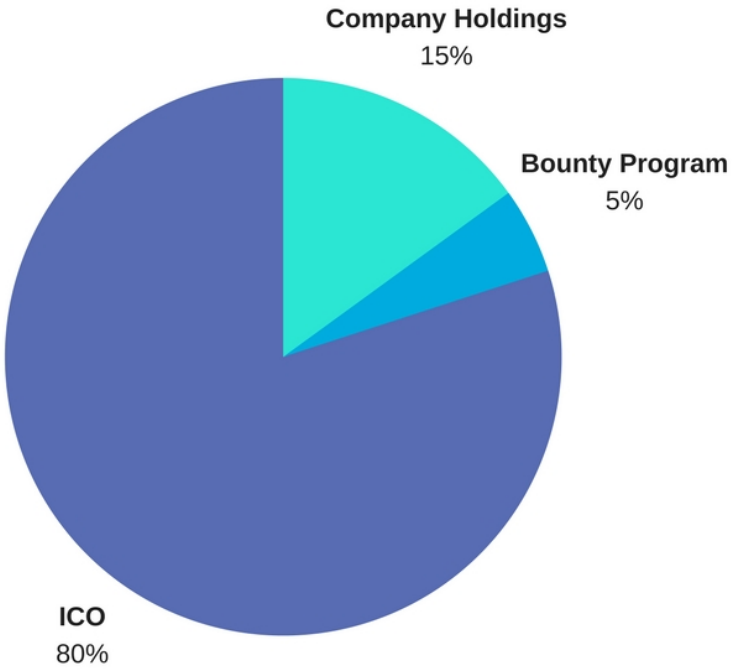
Then it's the ecommerce store's turn. They get a notification about a new pending transaction and send the handbag to Alison. After they've send the handbag they return to the Confido platform and submit the shipping information. Confido tracks the package and releases the money after it's been delivered.

THE TOKEN

The Confido token is a basic ERC20 token that has the same capabilities as most other ERC20 coins. The thing that makes Confido tokens valuable is the ability to earn Ether passively by holding tokens. Users that have invested in Confido tokens will receive 0.7% in ETH of the payments made through Confido. That means that investors will earn money simply by holding the token. Pay-outs are bimonthly.

TOKEN DISTRIBUTION

Our token distribution is quite simple.



Fifteen percent of all tokens created (2.250.000) will be held by the company to make sure we get at least 15% of the revenue created by transaction fees. Five percent (750000) will be kept aside for the bounty campaign. The remaining eighty percent (12.000.000) will be available in the ICO.

All unsold tokens in the ICO will be burned. We do this to increase the individual value of a token for our investors.

ICO information

Our ICO will start on the 14th of October. The hard cap will be $500,000. We want to keep our initial market cap low to ensure greater growth to our investors. The price of one Confido token will be $0.04.