Whitepaper v1.0.0

Secure Escrow Service and Private Solution
powered by Blockchain Technology

March 2021

Abstract

PayrLink is a decentralized application powered by Blockchain technology that works as a decentralized third-party arbitrates transactions in a private manner from very simple and highly complex ones. The result is a private solution and secure escrow service that renders ultimate judgements in a fast, inexpensive, reliable and decentralized way.

1. Introduction

It's hard to trust anyone these days, especially in a world where everything happens online. The days of meeting people, shaking their hands, doing a deal is a long gone. We need to feel safe and private when doing transactions online.

By default, the entire blockchain transaction history and balances are public. All transactions can be viewed on block explorers like Etherscan, and anyone who knows that you own a particular address can easily view your payments, trace the source of your funds, calculating your holdings, and analyze your on-chain activity.

But what if you did not want your history and balances to be publicly viewed by everyone? What if you wanted anonymity and privacy, when it came to your transactions?

This is where PayrLink comes into the world. We purpose to revolutionize the Escrow industry with private transactions backed by Blockchain technology for a fraction of the price of a conventional escrow service.

2. Decentralized Escrow Service

"Whoever controls the courts, controls the state". Aristotle.

- What is a decentralized escrow service?

In a conventional Escrow world, the Escrow company facilitates everything about the transaction: receiving the money, confirming the buyer has received their items or services, and releasing the funds to the seller. Processes like this can take a lot of time.

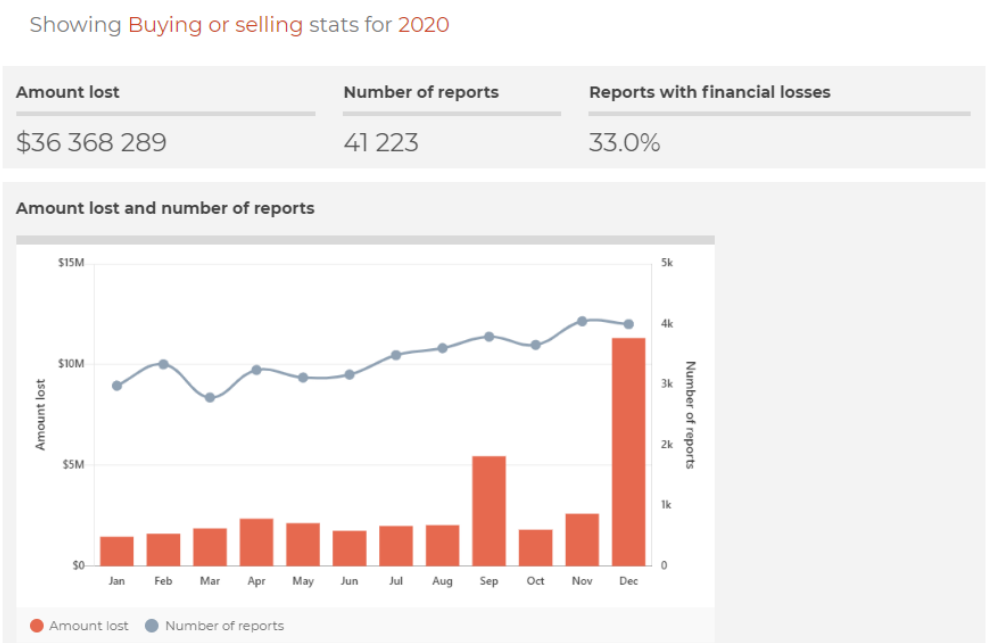
In a Decentralized Escrow world however, the major difference is the blockchain and smart contracts are the Escrow company. This makes the transactions exponentially quicker, much more secure and can cost a fraction of the price. There is no corruption and officials can't be bought.

For example: in a conventional escrow world, a simple domain transfer can take days for the seller to receive their money, but in a decentralized world that process could take a matter of hours.

- Industry Statistics

There has been an influx of online transactions between buyers and sellers over the past several years, but unfortunately there has also been an influx of fraud in online transactions.

The chart below shows the increase of "buying and selling" related fraud transactions recorded in Australia alone over the 2020.



https://www.scamwatch.gov.au/scam-statistics?date=2020&scamid=15

This fraud could have been avoided if a secure and trusted Escrow Service was used to facilitate the transactions. PayrLink prides itself in providing a secure service to help prevent the losses consumers otherwise would have faced due to fraud.

Smart contracts have to designate PayrLink as their arbitrator. When they opt-in, contracts creators choose how many jurors and which court will rule their contract in case a dispute occurs. The idea is that they will choose a type of court specialized in the topic of the contract. A software development contract will choose a software development court, an insurance contract will select an insurance court, etc.

- Juror votes

After assessing the evidence, jurors commit their vote on one of the options. Jurors have to stake their PAYR to PayrLink at least 1 month in advance to prove they are not related to the dispute. They submit hash (vote, address). The address is the address of juror. It is required in order to make the commitment of each juror different, thus preventing a juror from copying the commitment of another. When the vote is over, they reveal vote, and PayrLink smart contract verifies that it matches the commitment. Jurors failing to reveal their vote are penalized. Jurors who voted wrong, have to contribute a portion of their PAYR stake.

After a juror has made a commitment, his vote cannot be changed. But it is still not visible to other jurors or to the parties. This prevents the vote of a juror from influencing the votes of others. Jurors can still declare that they voted in a certain way, but it is challenging for them to provide other jurors a reason to think that what they say is true. This is an important feature for the Focal Point to arise. If jurors knew the votes of other jurors, they could vote like them instead of voting for the Focal Point.

As these two step processes of committing and then revealing one's vote requires additional user interactions, in some low stakes subcourts, one might want votes to be issued publicly to simplify the user experience.

- Arbitration Fee

In order to compensate jurors for their work and avoid an attacker from spamming the system, creating disputes and appealing requires arbitration fees. Each juror who is coherent with the final ruling will be paid a fee determined by the subcourt where the dispute is solved. The arbitrable smart contract will determine which party will pay the arbitration fee. The rules can be simple. We require the party creating the dispute or the party appealing to pay the fee.

Dispute Arbitration Fees will be distributed to jurors who take part in the subcourt.

- Common Transaction Fee

PayrLink takes a fraction of the total amount as a common transaction fee. Common transaction fees will be distributed to all jurors who have their PAYR stake on PayrLink.

3. A Use Case of Arbitrated Contracts

Alice is an entrepreneur based in United States. She hires Bob, a programmer from Mexico, on a P2P freelancing platform to build a new website for her company. After they agree on a price, terms and conditions, Bob gets to work. A couple of weeks later, he delivers the product. But Alice is not satisfied. She argues that the quality of Bob's work is considerably lower than expected. Bob replies that he did exactly what was in the agreement. Alice is frustrated. She

cannot hire a lawyer for a claim of just a couple hundred dollars with someone who is halfway around the world.

What is the contract had a clause stating that, should a dispute arise, it would be solved by a PayrLink court? After Bob stops answering her, Alice taps a button that says “Appeal to PayrLink” and fills a simple form explaining her claim.

Thousands of miles away, in China, Chief is a software developer. In his “dead time” on the bus commuting to his job, he is checking PayrLink Court Platform to find some arbitration work. He makes couple thousands of dollars a year on the side of his primary job by serving as a juror in software development disputes between freelancers and their clients. He usually rules cases in the Website Quality Subcourt. This court requires skills in HTML, JavaScript, and web design to solve disputes between freelancers and their customers. Chief stakes 20000 PAYR from 1 month ago, the token used by PayrLink to resolve disputes with proof of stake. The more tokens he stakes, the more likely is that his vote will be selected as a winner and he will get more arbitration reward.

Similarly, James, a programmer from England, and Momir, from Serbia, also staked their PAYR on the PayrLink and decided to take part in Website Quality Subcourt. They will never know each other, but they will collaborate to settle the dispute between Alice and Bob. On the bus back home, Chief analyzes the evidence and votes who is right.

Two days later, after the three juries have voted, Alice and Bob receive an email: “The jury has ruled for Alice. The website was not delivered in accordance to the terms and conditions agreed by the parties. A smart contract has transferred the money to Alice”. Jurors are rewarded for their work and the case is closed.

4. Private Solution with Zero Knowledge Proof

Over the years there have been many attempts at creating private transactions on Ethereum. Some workarounds trying to obscure value flows, like using a centralized mixing service, however, introduce a high degree of counterparty and surveillance risk. PayrLink uses various cryptographic methods including implementations of ZKP (Zero-Knowledge Proof) to achieve the privacy functionality.

In cryptography, a zero-knowledge proof or zero-knowledge protocol is a method by which one party (the prover) can prove to another party (the verifier) that they know a value x, without conveying any information part from the fact that they know the value x. The essence of zero-knowledge proofs is that it is trivial to prove that one possesses knowledge of certain information by simply revealing it; the challenge is to prove such possession without revealing the information itself or any additional information.

If proving a statement requires that the prover possesses some secret information, then the verifier will not be able to prove the statement to anyone else without possessing the secret information. The statement being proved must include the assertion that the prover has such knowledge, but not the knowledge itself. Otherwise, the statement would not be proved in zero-knowledge because it provides the verifier with additional information about the statement by the end of the protocol. A zero-knowledge proof of knowledge is a special case when the statement consists only of the fact that the prover possesses the secret information.

Interactive zero-knowledge proofs require interaction between the individual (or computer system) proving their knowledge and the individual validating the proof.

A zero-knowledge proof must satisfy three properties:

- Completeness: if the statement is true, the honest verifier (that is, one following the protocol properly) will be convinced of this fact by an honest prover.
- Soundness: if the statement is false, no cheating prover can convince the honest verifier that it is true, except with some small probability.
- Zero-knowledge: if the statement is true, no verifier learns anything other than the fact that the statement is true.

PayrLink improves transaction privacy by breaking the on-chain link between recipient and destination addresses with Zero Knowledge Proof. It uses a smart contract that accepts deposits that can be withdrawn by a different address.

To make a deposit user inputs destination address and sends its hash (called a commitment) along with deposit amount to the PayrLink smart contract. The contract accepts the deposit and adds the commitment to its list of deposits.

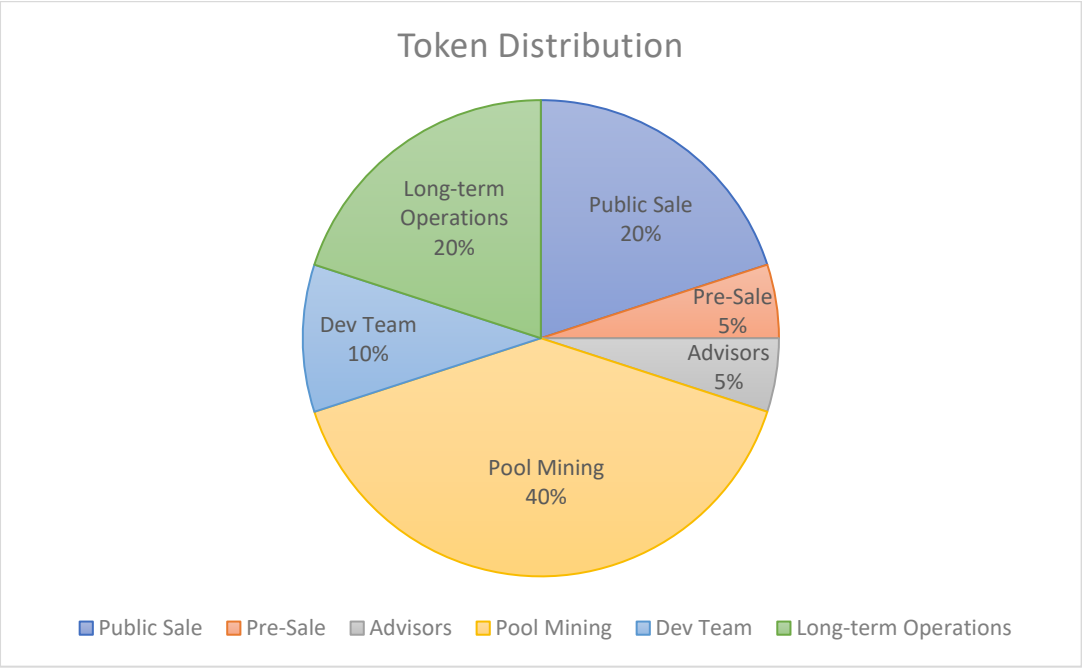
Later, the user decides to release the funds to the destination address. In order to do that, the receiver should provide proof that he or she possesses an address to a commitment from the smart contract's list of deposits.

Once the receiver provides the proof, the funds become the deposit of the receiver and he can send it again to another address in a private manner.

5. Incentive Advantages

	PayrLink	NAT	Escrow	MangoPay	ShieldPay
Use of Crypto	Yes	Yes	No	No	No
Transaction Fee	0.8%	1~3%	1~6%	1.8%	1.5~3%
Dispute Arbitration Fee	1.2%	1.2%	1~2%	1~2%	1~2%
Decentralized Voting Arbitration	Yes	Yes	No	No	No

6. Tokenomics



A total supply of 200,000,000 PAYR will be created and 50,000,000 PAYR will be made available for sale during the initial token sales.

There will be no softcap, meaning the project will continue despite the amount raised. The basic principle which has been observed in distribution policy is implementing maximum dispersion and avoiding centralization.

10% of tokens are dedicated to founder team of PayrLink and 5% of tokens are distributed to our advisors.

7. Conclusion

We have introduced PayrLink, a decentralized escrow and private solution powered by Blockchain technology. You can see summary and technical introductions in this paper.

The rise of the digital economy created labor, capital and product markets that operate in real time across national boundaries.

Cryptocurrencies are giving many the possibility of having their first bank account to send and receive money in a secure and private way. Cryptocurrencies are helping millions achieve financial inclusion. PayrLink will do the same in access to justice by enabling arbitration in a large number of contracts that are too costly to pursue in court in a private manner. Just as Bitcoin brought “banking for the unbanked”.